

Applicant Privacy Notice (APN)

Effective date: August 2022

Nagarro understands the importance of your privacy. “Nagarro” (hereinafter also referred to as “we” or “us”) is a group of companies operating worldwide, a list of which can be found at <https://www.nagarro.com/en/contact-us>. All of them act as joint controllers for the processing activities described in this Applicants Privacy Notice (“APN”) in the sense of Art. 26 EU General Data Protection Regulation (GDPR). We are committed to respecting your privacy and protecting your personal data, which is any information that can identify you as an individual person. This APN provides you with information on how we handle and protect your personal data when registering for our careers portal online on SmartRecruiters and/or applying for a job at Nagarro.

This Privacy Notice applies only to the personal data of job applicants, potential candidates for employment, and participants in any other recruiting programs and events etc. It does not apply to our employees, contractors or clients, or other personal data that Nagarro collects for other purposes.

Personal data we collect

We usually collect personal data directly from you, when you register for our career portal and/or apply for a position with us, such as your name, contact details, address, work and educational details and test results. The information we request from you may vary depending on the jurisdiction for which you apply. We also may collect personal data about you from third parties, such as professional recruiting agencies, your references, prior employers, or Nagarro employees with whom you have interviewed. In some jurisdictions, this may include information from background check agencies, to the extent this is permitted by applicable law (the data categories to be checked being, for example, identity and contact data, educational qualification data and skill and professional experience data etc.).

When you visit our website and/or register for our career portal we may obtain such information as is required to provide the web service (e.g. IP address, date and time of access, browser type, and operating system). For more information see <https://www.nagarro.com/en/privacy-policy>.

Sensitive personal data is a subset of personal data and includes ethnicity, health, trade union membership, philosophical beliefs, sexual orientation, as well as other categories as prescribed by law. We do not seek to obtain and will not collect such data

about a candidate unless permitted or required to do so by applicable laws (e.g. because equal opportunity monitoring or tax laws require it).

Use of your personal data

We process your personal data for the following purposes:

- administering your registration with our career system;
- administering your application, which may include evaluating your skills, organizing and conducting interviews and other steps necessary to potentially entering into an employment contract;
- recordkeeping in relation to recruiting and hiring;
- internal administrative purposes;
- using aggregated or anonymized/pseudonymized data to analyze and improve our recruiting process;
- ensuring compliance with legal requirements, including diversity and inclusion requirements and practices;
- conducting criminal history checks (for offences related to confidentiality breach, forgery, corruption etc.) in as far as permitted by applicable law (in some jurisdictions this may require consent which we would then obtain);
- protecting our legal rights to the extent authorized or permitted by law;
- disclosure or transfer of personal data in the event of a re-organization, merger, sale, joint venture, assignment, or other transfer or disposition of all or any portion of our business; or
- emergency situations where the health or safety of one or more individuals may be endangered.

The legal justification for the processing is the legitimate business interest of the joint controllers. In all of the above cases, we carefully assess the interests or fundamental rights and freedoms that you may have and balance them against the business interest.

In as far as the job application is for a specific job or required for the web service that you requested the processing may also be justified by contract performance concerning the specific group company.

In some cases we may be legally required to continue to process personal data, e.g. in case of record keeping for tax or corporate law reasons. Or, additional legal justifications may apply, e.g. because processing is required to comply with a legal obligation including any court or administrative orders; or in case the processing is required to protect the vital interests of a data subject; or processing is necessary for the performance of the tasks carried out in the public interest.

Data recipients and international data transfers

Your personal data may be accessed by recruiters and interviewers with a need-to-know depending on the job that you apply for and your choice of recruiting program (global, geo-specific or job specific). Individuals performing administrative functions and

IT personnel within Nagarro may also have a limited access to your personal data to perform their jobs.

We use third party service providers to provide a recruiting software system with EU-based data storage. We may also share your personal data with other third-party service providers that may assist us in recruiting talent, administering and evaluating pre-employment screening and testing, and improving our recruiting practices. We maintain processes, including data processing agreements, designed to ensure that any processing of personal data by third party service providers is consistent with this APN and protects the confidentiality, availability and integrity of your personal data.

We may transfer your personal data to countries outside the country in which you reside. This may include countries which may not provide the same level of data protection available in your jurisdiction. For this, we have put in place legal mechanisms designed to ensure adequate data protection of your personal data that is processed by Nagarro subsidiaries and affiliates within the Nagarro globally and with third party providers, including the transfer of your personal data to countries other than the one in which you reside. Where required by law, we put in place legal mechanisms designed to ensure adequate data protection of your personal data in a third country. If you would like more information about these legal mechanisms, which may include the EU's Standard Contractual Clauses, please contact us at the address provided at the end of this document.

Data retention

If you accept an offer of employment from us, any relevant personal data collected during your pre-employment period will become part of your personnel records in the organization and will be retained in accordance with specific country requirements. The periods for which your data will be held will be provided to you in a new privacy notice, at the time of employment. If your application for employment is unsuccessful, Nagarro will usually hold your data on file for another 6 (six) to 12 (twelve) months after the end of the relevant recruitment process to protect our legal rights in case of any potential claims, according to the various requirements per jurisdiction. At the end of that period, or once you withdraw your consent, your data is not processed any longer.

The same mechanism for providing consent is meant to be used for withdrawing consent.

You can address any concerns regarding the processing of your personal data for recruitment purposes by contacting us at dpo@nagarro.com.

Security

We have implemented generally accepted standards of technical and operational security to protect personal data from accidental or unlawful destruction, loss, alteration, as well as unauthorized disclosure or access.

Your Rights

As a data subject, you may have the following rights under applicable law:

- Right of access, which means the right to obtain confirmation from us as to whether we are processing personal data about you, and, where that is the case, to access the personal data.
- Right to rectification, which means the right to ask us to rectify personal data you think is inaccurate. In addition, you have the right to ask us to complete personal data you think is incomplete.
- Right to erasure, which means the right to ask us to erase your personal data in certain circumstances.
- Right to restriction of processing, which means the right to ask us to restrict the processing of your personal data in certain circumstances.
- Right to object to processing; which means the right to object to processing if we process this personal data based on legitimate interests. Where personal data are processed for direct marketing purposes, you generally have the right to object to the processing for such marketing at any time.
- Right of data portability, means the right to ask that we transfer your personal data to you or another organization. This will only apply to personal data you have given to us and that we process based on your consent or for contract purposes.
- Right to withdraw consent, i.e. in case processing of your data is based on your consent, you have the right to withdraw that consent at any time, without affecting the lawfulness of any processing before the withdrawal.

We do not make recruiting or hiring decisions based solely on automated decision-making.

To help protect your privacy and security, we will take reasonable steps to verify your identity before granting e.g. access to your personal data. We will make reasonable attempts to promptly investigate, comply with, or otherwise respond to your requests, as may be required by applicable law. Depending upon the circumstances and the request, we may not be permitted to provide access to personal data or otherwise fully comply with your request. We reserve the right to charge an appropriate fee for complying with your request where allowed by applicable law, and/ or to deny your requests in case your request is unfounded, excessive or otherwise unacceptable under applicable law.

In addition, and where granted by applicable law, you may have the right to lodge a complaint with a competent data protection authority. For Nagarro companies established in the EU/EEA, you can find a list of the contact details of the competent EU data protection authorities here https://edpb.europa.eu/about-edpb/board/members_en.

CONTACT/JOINT CONTROLLERS

All Nagarro group entities act as joint controllers in the sense of Art. 26 EU General Data Protection Regulation (GDPR) and are jointly responsible for complying with GDPR requirements. If you have any questions about this APN or would like to exercise

Your Rights, please contact us at: **dpo@nagarro.com** (designated contact point). This is regardless of your right under GDPR or any other applicable law to contact each controller individually to exercise Your Rights. For example, if you want to contact the data protection officer or data protection contact of a specific Nagarro entity direct, you will find their contact details at <https://www.nagarro.com/hubfs/NagarroWebsiteRedesign-Aug2020/Assets/Docs/DPO%20List.pdf>

This Applicant Privacy Notice is effective as of August 2022.
