Applicant Privacy Notice (APN)

Effective date: March 2024 **Version**: 5.0

Introduction

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 Contact us | Nagarro). All of them act as independent controllers for the processing activities described in this Applicant Privacy Notice (“APN”).

We are committed to respecting your privacy and protecting your personal data. This APN provides you with information on how we handle and protect your personal data when you are going through the recruitment process at Nagarro.

This Applicant 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.

Categories of Personal data we collect

We usually collect personal data directly from you, when you register on our career portal and/or apply for a position with us.

- **Identification** - Name, Email, Phone number, Place of Residence, Government-issued identification document (only at the time of offer release, as applicable per jurisdiction)
- **Educational Details** – Institute Name, Details of education
- **Experience details** – Previous Employers, Title, Job Location, Resume
- **Interview details -** Video recording, Assessment test score and Interview feedback, etc.
- **Job professional site** – Links to online profile
- **Diagnostic data** -IP address, device information, this data is captured automatically

The information we request from you may vary depending on the jurisdiction from which you apply.

We may also record technical interviews for legitimate purposes such as identifying fraud in case someone is impersonating a candidate during the interview. For certain jurisdictions (EU, EEA and UK), the candidate's consent is sought before video recording, if a candidate does not provide consent, the interview process will continue without suffering any negative consequences in regards to the recruitment process.

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 may require it).

Category of the sources of the personal data

We may collect personal data through various sources. Most of the data is obtained directly from you when:

- You apply for a job yourself on our website and/or job portals (details are available in the Cookie Policy).
- You directly contact/email our official contact. ○ You share details with Nagarro employees for referrals.

The other sources of personal data are mentioned below:

- Sourced by Nagarro's affiliates, newly acquired entities.
- Sourced by our suppliers, vendors and service providers for recruitment purposes.
- Sourced from job sites and job boards, including your publicly accessible profiles.

Use of your personal data

We process your personal data for the following purposes:

- administering your registration with our recruitment system.
- administering your hiring process, 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.
- preventing fraud during the interview process such as impersonation.
- internal administrative purposes.
- using aggregated or anonymized/pseudonymized data to analyze and improve our recruiting process.
- ensuring compliance with legal obligations, including diversity and inclusion requirements and practices.
- conducting background verification check / 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.

Legal basis of the processing

The applicable privacy and data protection laws provide for certain justifiable grounds for the collection and processing of personal data, commonly referred to as the legal basis of processing. We primarily rely on the following legal bases:

- **Performance of a Contract** – For administrating job applications, we process your Personal Information when it is necessary for the performance of a contract to which you are the party or in order to take steps at your request prior to entering into a contract.

- **Legitimate interest** – To prevent fraud and conduct background verification, we process your Personal Information when it is necessary for a legitimate purpose.

- **Consent** – We may process your Personal Information with your consent for certain activities such as for video recording, as applicable per jurisdiction.
- **Legal Obligation** – To ensure compliance with legal requirements, we may process your personal information to comply with any applicable Legal obligations.
- **Vital Interest** – For emergency situations, we may process your personal information to protect your vital interests such as health and safety.

Data recipients, transfer, and disclosure of Personal Information

We may share your personal data with the following recipients:

- Nagarro and its affiliates
- Other third-parties who may assist us in administrating, and evaluating pre-employment, screening and testing and improving our recruitment practices.
- Auditors, and or government authorities, where applicable
- Customer for specific hiring

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 outside the country in which you reside. This may include countries that may not provide the same level of data protection available in your jurisdiction. We shall take reasonable and appropriate steps in line with applicable laws while executing such transfer. 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.

We don’t disclose/share/sell your personal data to any third parties who are not required to receive your data for the purposes mentioned above.

Data Storage and retention

We use third-party service providers to provide a recruiting software system with EU-based data storage.

If you accept an offer of employment from us, any relevant personal data collected during your preemployment 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.

We will not retain your personal data for more than what is necessary to fulfil the aforementioned purposes. Once you request for your data to be deleted, we will stop your data from being processed any further, however, for business purposes, the data will be retained for 6 months from the last activity date on your application before it will be securely disposed of. During these 6 months, you may choose to apply for another job which will cancel your deletion request.

Post the retention period, data is automatically deleted from the Recruitment system and it wipes out all the details of the previous interactions from the recruitment system.

Security of your personal data

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 personal data may be accessed by authorized recruiters and interviewers based on the need-toknow principle (depending recruiting program such as global, geo-specific or job specific).

When conducted, the video recordings are kept strictly confidential, under strict access controls, and not shared with any third party for any further sub-processing.

Your Data Privacy Rights

Subject to the laws of your country, you may have certain rights as a data subject (including but not limited to right to information, access, rectification, erasure, object, restriction of processing, right to lodge a complaint with a supervisory authority, relating to your Personal Information that we process).

Our Recruitment software provides a mechanism for you to access your profile and modify your personal information when required. It also provides a mechanism to delete your profile, however, you may reapply for another position which will cancel your deletion request.

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

To help protect your privacy and security, we will take reasonable steps to verify your identity before taking steps to execute your rights e.g. access to your personal data. When we receive your request, 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.

If you are unhappy with how we safeguard your personal data, depending on the laws of the countries where you reside, you have the right to bring a complaint to your local data protection authority.

Modification of the policy

Nagarro reserve the right to make change to the data privacy practices and update this privacy notice if there are any changes required. However, our commitment to uphold your privacy and protect your data will remain.