

## Privacy Notice for Recruitment Candidates

*Last updated: April 7, 2025*

nexus.ai Group of companies (entities that are affiliated and belong to the same corporate group of entities, including, but not limited to **UAB Spectra tech**, a private limited liability company organized under the laws of Lithuania, registration number 307041682, having its registered office at Švitrigailos str. 36, Vilnius, Lithuania; **harmony sp. z o.o.**, a private limited liability company organized under the laws of Poland, registered address ul. Złota 59, 00-120 Warsaw, Poland; **nexus B.V.**, a private limited liability company organized under the laws of the Netherlands, under registration number 867238069, registered address Fred. Roeskestraat 115, 1076 EE Amsterdam, the Netherlands) (together referred to as “**nexus.ai**”, “**we**”, “**us**”, or “**our**”) are committed to protecting and respecting your privacy.

In addition, this Privacy Notice for Recruitment Candidates (together with any other documents referred to herein, collectively, the “**Notice**”) sets out the basis on which the personal data collected from you (as prospective employee/worker), or that you provide to us, will be processed by us in connection with our recruitment processes. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

This Notice provides you with certain information that must be provided under the General Data Protection Regulation (EU) 2016/679 (“**GDPR**”) and the local data protection laws. Please note that the California Consumer Privacy Act (“**CCPA**”) includes concepts similar to the GDPR: for example “business” is similar to “data controller”. For simplicity, when we talk about nexus.ai being a “data controller”, we also mean that nexus.ai is a “business” in the sense of CCPA. Also, as per definitions in the CCPA, please note that nexus.ai does not sell, share, lease, or rent your personal information.

## PROCESSING OF YOUR PERSONAL DATA

We collect and use your personal data for recruiting purposes – in particular, to:

- Manage the hiring process and communicate with you about it.
- Consider you for, and assess your suitability for, employment opportunities with us.
- Verify your information and carry out background checks (to the extent permitted by applicable laws).
- Make a hiring decision.
- Inform the referrer of the status and final outcome of your application (if you were referred).
- Stay in touch and engage with you.
- Maintain and improve our recruiting processes.
- Comply with legal or regulatory requirements.
- Deal with any legal disputes involving you or other prospectives.
- Transfer our business (we may share your personal data in those cases where we sell or negotiate to sell our business or go through a corporate merger, acquisition, consolidation, asset sale, reorganization, or similar event). In these situations, nexos.ai will continue to ensure the confidentiality of your personal data.

## PERSONAL DATA PROCESSED

The main personal data categories and the data which is processed by us for the purposes mentioned above are the following:

- **Identification and contact information, and related identifiers** such as your full name, age or date of birth, gender, pictures, address or the place of residence, email address, phone number, etc.

- **Professional or employment-related information**, which may include nationality/visa/right to work permit information, languages you speak and level of proficiency, computer/technical skills, background screening results, etc.
- **Career information** such as job titles, work history, performance information, information about qualifications, professional memberships, disciplinary and grievance information, etc.
- **Education information** such as institutions/trainings/courses/seminars attended, degrees, certifications, licenses held, publications, etc.
- **References** such as our employees or your named referees and/or former/current employers feedback/references/referrals, etc.
- **Information about interaction with us** such as email communication, information about expected salary and other job preferences, records of interviews and tests/assignments or assessments, information indicated in motivation/covering letters, CCTV recordings made in our premises if you visit us at our premises, professional social media accounts, etc.
- **Other information** such as any information you voluntarily choose to provide in connection with your job application.

In exceptional circumstances, we may also collect, store and use the following types of more sensitive information, for example, gender, marital status, race/ethnicity, the existence of disability, or health condition. We may process the mentioned data where necessary for the establishment, exercise, or defense of a legal claim by us, with your explicit consent, or where necessary for the purpose of carrying out our legal obligations in the context of an employment or social security law. However, please do not voluntarily disclose your personal identification numbers or any other sensitive personal information, such as health information, information on family relations or similar, that is not necessary for the recruitment process in the communication/submitted documents.

In some cases, we may also need to collect information about candidates' administrative offenses (if any). If this is the case, we will do this only in accordance with applicable legal requirements. We will always explain before the collection of such information why we need it and seek your consent (if this is required by law).

Please note that if you are unwilling to provide your personal data to support our recruitment and/or evaluation process, we may not be able to process your application properly or at all.

## **GROUNDINGS FOR PROCESSING OF PERSONAL DATA**

Our legal basis for collecting and using the personal data described in this Notice will depend on the personal information concerned and the specific context in which we collect and use it:

- We will normally process your personal data in order to prepare and enter into an employment contract with you (if you accept our offer).
- Where the processing is in our (or others) legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms (for example, assessing your application, managing and improving our recruitment and hiring processes).
- When processing is necessary for carrying out our obligations and exercising our rights in the field of employment, social security or social protection law (for example, information about your physical or mental condition may be collected in order to consider accommodations we need to make for the recruitment process and/or subsequent job role).
- Where we have your consent to process your personal data, which you may revoke at any time (for example, to contact you for our future employment opportunities).
- In some cases, we may also have a legal obligation to collect personal information from you or may otherwise need the personal information to protect a substantial public interest or your vital interests or those of another person (for example, to protect the security of you or others).

## PERSONAL DATA SOURCES

In general, we get your information directly from you. However, we may also obtain personal data about candidates from the following sources:

- Job search portals (such as cvbankas.lt, cvonline.lt) and/or recruiting agencies.
- Background screening agencies.
- Employment-oriented social media sites, sources and/or collaboration platforms (such as LinkedIn). If we collect any information from your social media profiles, we make sure that it is relevant to the job position you applied for. We base the collection of data from social media profiles on our legitimate interest to assess specific qualities for specific job functions.
- From any other company representing the nexus.ai brand.
- Our employees (referrals), if they have referred you.
- Your named referees and/or former/current employers. Please note that we obtain your personal data from your current employer only if we have your separate consent for this.

## PERSONAL DATA SHARING AND TRANSFERS

We share personal data globally, both internally within the companies representing the nexus.ai brand, and externally with our third-party partners/service providers:

- **Other nexus.ai group companies.** Companies representing the nexus.ai brand share infrastructure, systems, web hosting, and technology to ensure efficiency, business continuity, and security, as permitted by applicable law, and in accordance with this Notice. For example, nexus.ai recruiters collaborate globally to connect candidates with the right opportunities. If we see that you would make a great candidate for an open position at another company representing the nexus.ai brand, we may share your application with a responsible HR representative.

- **Service providers.** We work with various third-party partners who help us manage and improve our recruiting process, including tools and systems we use for this purpose. These third parties include recruitment agencies, vendors facilitating interviews/tests, relocation and/or immigration advisors (where applicable), applicants tracking software providers (such as Lever Inc. (USA), reporting and analytics service providers, vendors facilitating pre-employment screening services, video conferencing tools providers (such as Zoom Video Communication, Inc., Microsoft Corporation), IT developers and support providers, cloud computing services providers (such as Google Ireland Ltd., Google LLC (USA), project management software providers, third parties who provide support and advice including in relation to legal, financial/audit/business management/insurance/health and safety/security issues, etc.
- **Courts and/or governmental/law enforcement authorities.** We may disclose personal data to establish or exercise our legal rights or defend against any legal claims or other complaints. We can also respond to legal requests when we have a belief that the response is required by law in that jurisdiction.

We require the above-mentioned third parties to protect the personal data they receive with appropriate security measures and prohibit them from using the personal data for their own purposes or outside what is necessary to provide the service. Please note that sometimes your personal information may be processed in countries where these providers are based, including locations that may not guarantee the same level of protection of personal data as the one in which you reside. We assess the circumstances involving all cross-border data transfers and have suitable safeguards in place to require that your personal data will remain protected in accordance with this Notice. For example, in case your personal data is transferred to countries outside the EEA, we make sure there is an adequacy decision from the European Commission with regards to the recipient country or we use standard contractual clauses approved by the European Commission for such transfer of your personal data.

## **YOUR RIGHTS IN CONNECTION WITH PERSONAL DATA**



Please note that there are various data protection laws across different jurisdictions that provide privacy rights to you as a data subject. Subject to those applicable data protection laws, among others, you may have the following rights:

- **Delete:** request us to erase your personal data.
- **Access:** know and access personal data nexos.ai has collected about you.
- **Rectify:** rectify, correct, update, or complement inaccurate/incomplete personal data nexos.ai has about you.
- **Object:** object to the processing of your personal data which is done on the basis of our (or others) legitimate interests.
- **Transfer:** request us to provide you with a copy of your personal data in a structured, commonly used, and machine-readable format or to transmit (if technically feasible) your personal data to another controller (only where our processing is based on your consent and carried out by automated means).
- **Restrict:** restrict the processing of your personal data (when there is a legal basis for that).
- **Withdraw consent:** withdraw your consent where processing is based on consent you have previously provided.
- **Lodge a complaint:** exercise your rights by contacting us directly or, if all else fails, by lodging a complaint with a supervisory authority in your country. A list of contact details for supervisory authorities in the EEA is available [here](#), for the Swiss authority – [here](#), and for the UK data protection authority – [here](#).

If you want to exercise your rights (or have any questions/comments), you can always reach out to the recruiter handling your application or contact us at [legal@nexos.ai](mailto:legal@nexos.ai).

If we have reasonable doubts regarding the identity of the individual submitting the request, we may request additional information necessary to verify your identity. We will make every effort to

respond to your request within one month. However, please be aware that this period may be extended by an additional two months in certain circumstances.

## PERSONAL DATA SECURITY

We maintain tight controls over the personal data we collect. Our dedicated IT security team has implemented appropriate physical, technical, and organizational measures to protect information about you against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access and against all other unlawful forms of processing:

- **Physical Measures.** We control access to our facilities with access cards. We also use security alarm systems and CCTV. We store devices with personal data information only in locked rooms or cabinets. Our printers are protected by access control measures. A clean desk policy is implemented.
- **Technical Measures.** We use layered defense with firewalls, anti-malware protection, intrusion detection, and prevention systems. Our infrastructure is regularly updated and regular vulnerability scans are in place to detect possible vulnerabilities. We have security event and incident management solutions to correlate and investigate signals in security tools. Servers are hardened and automated configuration tools are used to manage them. All workplaces are managed from a centralized endpoint management tool. Data at rest and in transit are encrypted. Encryption protocols are used according to the newest security practices.
- **Organizational Measures.** We adopted information security and data processing policies according to best practices. We have external audits to prove our information security and data processing policies are up to standards. We adopted a constant development culture of security and data protection awareness among our employees (including organizing regular and ongoing training and other awareness activities). We analyze the threat landscape and attack surface and constantly update our security



measures. Access to databases containing personal data is granted on a need-to-know basis.

If we detect something suspicious, we will notify you immediately and guide you through steps to stay better protected. However, no company can guarantee the absolute security of internet communications as no technology is completely bulletproof. If you have any reason to believe that your interaction with us is no longer secure, please notify us at [legal@nexus.ai](mailto:legal@nexus.ai).

## **PERSONAL DATA RETENTION AND DELETION**

nexus.ai will store the personal data about the candidate for as long as the selection to the specific position is taking place and 1 (one) year after, if longer terms are not required in order to comply with our legal obligations and/or to resolve disputes (e.g., to demonstrate non-discriminatory practices or to confirm the fairness and transparency of our recruitment procedures). If you become our employee, we will save your recruitment information as part of your employee records under nexus.ai's employee personal data processing policy.

Sometimes, if we choose another candidate or you reject our offer, we may request your separate consent for the purposes of future recruitment processes. Such personal data will be stored for 3 (three) years following the receipt of your consent or until the day you withdraw your consent.

## **CONTACT US**

For any questions concerning our processing of your personal data please reach out to the recruiter handling your application or contact us at [legal@nexus.ai](mailto:legal@nexus.ai).

## **CHANGES**



We may update this Notice from time to time to reflect changes in legal, regulatory and operational requirements, our recruitment practices, and other factors. Please check this Notice frequently on our website for updates.