JOB CANDIDATE PRIVACY NOTICE

This Job Candidate Privacy Notice ("**Notice**") describes what personal data Mobilesson Ltd. d/b/a Connecteam, and our affiliates ("**Connecteam**", "**we**" or "**us**"), collect and process regarding our job candidates and applicants ("**Candidates**", "**you**" or "**you**") with respect to our application and recruitment process, why we collect it and how we use it. It also describes how candidates may exercise their rights to such data held with us.

We strongly urge you to read this Notice and make sure that you fully understand and agree to it. If you do not agree to this Notice, please avoid providing us with your data.

You are **not** legally required to provide us with any personal data, but without it, we may not be able to process your application.

1. What data do we collect and how we collect it?

Throughout the application and recruitment process, you may provide us (or we may otherwise have access to) personal data about you, such as your identifying data, contact details, resume/CV, work-related data, social media activity, etc. We may collect this data directly from you, as you provide it voluntarily through your application and candidacy review process, or from other sources such as recruitment agencies, background check services (as applicable and subject to applicable law), or your references.

We may use such data to assess our Candidates' skills and qualifications, and overall to verify, consider and process their application and candidacy for any of our positions, and to communicate with them regarding such processes. We may also use it to manage risk and enhance our security and anti-fraud measures, and to create aggregated statistical or inferred data regarding our Candidates for further development and improvement of our recruitment processes.

In addition, we may use personal data to act as permitted or required by any legal or regulatory requirements. Shall we wish to conduct any additional activities that may require the use of your data, we will notify you in advance and, if required by applicable law, request your prior specific consent.

In some regions, we may also require you to submit sensitive data relating to your ethnicity, gender, and whether you have a disability, to ensure our compliance with our legal obligations under applicable law. We may also collect sensitive data about your prior criminal convictions and offences as part of our background checks for specific roles if permitted or required by law. To the extent legally required, we will obtain your explicit consent prior to any such collection and use.

2. For what purposes do we use your data?

We will use and process your personal data as part of the employment application process at Connecteam for the following purposes and in reliance on the lawful bases detailed below:

Purpose	Lawful Basis for Processing
To evaluate your suitability for a role at Connecteam, and progress your application	▪ Performance of a Contract
To contact you about other suitable roles within Connecteam in the future	▪ Legitimate Interests ▪ Consent (where applicable)
To maintain our internal records of recruitment and employment applications	▪ Legal Obligations ▪ Legitimate Interests
To create your employee personnel file, if hired	
To comply with applicable legislation and industry codes	
To manage risk and enhance our security and anti-fraud measures	▪ Legitimate Interests
To further develop and improve our recruitment processes	

To protect the rights and interests of Connecteam and its affiliates	

If you reside in a territory governed by privacy laws under which "consent" is the only or most appropriate legal basis for the processing of personal data as described herein, your acceptance of this Notice will be deemed as your consent to the processing of your personal data for all purposes detailed in this Notice. If you wish to revoke such consent, you may do so at any time by contacting us at dpo@connecteam.com.

3. Where do we store your data?

Your personal data will be maintained, processed and stored by Connecteam and our Service Providers (as defined in Section 6 below) in Connecteam's different offices worldwide, including in Israel and the US, in the applied position's location(s), and other jurisdictions, as necessary for the proper handling of your candidacy.

While privacy laws may vary between jurisdictions, Connecteam, its affiliates and Service Providers processing personal data on our behalf are each committed to protect personal data in accordance with this Notice, customary industry standards, and such appropriate lawful mechanisms and contractual terms requiring adequate data protection, regardless of any lesser legal requirements that may apply in the jurisdiction to which such data is transferred.

To the extent we transfer Candidates' personal data originating in the European Economic Area (EEA), UK, or Switzerland to countries that have not been recognized as offering an adequate level of data protection by the relevant competent authority, we rely on appropriate contractual undertakings and data transfer mechanism as established under applicable law, such as the standard contractual clauses adopted by the EU (available here) and the UK (available here). If we transfer Candidates' personal data originating from the EEA to Israel or the UK, and if we transfer such data originating from the UK to Israel or the EEA, we rely on the respective adequacy findings of the EU and the UK regarding the level of data protection offered by Israel, the UK, and the EEA.

4. How long may we keep your data for?

We may retain Candidates' data even after the applied position has been filled or closed. This is done so we could reconsider Candidates for other positions and opportunities at Connecteam; so that we may use their personal data as reference for future applications submitted by them; in case the Candidate is hired, for additional employment and business purposes related to their work; and as reasonably necessary to comply with our legal obligations, to resolve disputes, prevent fraud and abuse, enforce our agreements or otherwise protect our legitimate interests.

5. How do we secure your data?

Connecteam has implemented industry standard security measures designed to protect the personal data of our candidates, including physical, procedural, and electronic measures. We also regularly seek new ways and tools for further enhancing the security of our system and the integrity of the personal data that we hold. Please be aware that regardless of the measures we take and the efforts we make, we cannot and do not guarantee the absolute protection and security of any personal data stored with us.

6. Who will have access to your data?

Connecteam will share your personal data with several selected Service Providers, whose services and solutions complement, facilitate and enhance our own. These include any recruitment firms that have referred you to us (or vice versa), candidate evaluation centers, recruitment software providers, background checks providers, data and cybersecurity services, web analytics, and our business, legal, compliance and financial advisors (collectively, "**Service Providers**"). Such Service Providers may receive or otherwise have limited access to our Candidates' personal data, depending on each of their particular roles and purposes in facilitating and enhancing our recruitment process, and may only use it for such purposes.

Additionally, we may disclose or otherwise allow access to any Candidates' personal data pursuant to a legal request, such as a subpoena, search warrant or court order, or in compliance with applicable laws, with or without notice to you, if we have a good faith belief that we are legally required to do so, or that disclosure is

appropriate in connection with efforts to investigate, prevent, or take action regarding actual or suspected illegal activity, fraud or other wrongdoing. We may also share your personal data with others, with or without notice to you, if we believe in good faith that this will help protect the rights, property or personal safety of Connecteam, any of our customers or employees, or any member of the general public.

Finally, we may share personal data internally within our family of companies, for the purposes described above. In addition, should Connecteam undergo any change in control, including by means of merger, acquisition or purchase of all or part of its assets, your personal data may be shared with the parties involved in such event.

7. Which cookies and tracking technologies do we use?

Connecteam uses certain monitoring and tracking technologies, such as "cookies" and other downloaded data files, including ones offered by our Service Providers. These technologies are used to maintain, provide and improve our processes and operations on an ongoing basis, and in order to provide a better experience to our website visitors and Candidates.

For example, these technologies enable us to better secure our website and services and detect abnormal behaviors, to identify technical issues, and to monitor and improve the overall performance of our services and processes.

To learn more about our cookies practices, please visit our Cookie Policy.

8. How can you exercise your rights?

If you wish to exercise your privacy rights under any applicable law, including the right to request access to, and rectification or erasure of, your personal data held with Connecteam; to port it or to restrict its processing; to object at any time to any processing of your data which is based on our legitimate interests (as detailed in Section 2 above); or to exercise any similar rights afforded to individuals under the laws that apply to you, you may do so by contacting our Data Protection Officer (DPO) at dpo@connecteam.com.

Please note that we may require additional information, including certain personal data, in order to authenticate and process your request. Such additional information may then be retained by us for legal purposes (e.g., as proof of the identity of the person submitting the request), in accordance with Section 4 above.

Please also note that such rights are not absolute. There are instances where applicable law or regulatory requirements allow or require us to refuse to provide some or all of the personal data that we hold about you. In the event that we cannot accommodate your request, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Additionally, you have a right to lodge a complaint with a competent data protection authority, such as the supervisory authority in the EU Member State of your habitual residence, place of work, or of the alleged GDPR infringement, the UK's Information Commissioner's Office, or your State's Attorney General (as relevant and applicable).

9. California requirements

This policy describes the categories of personal information we may collect and the sources of such information (in Section 1 above), and our retention (Section 3) and deletion (Section 7) practices. We also included information about how we may process your information, which includes processing for "business purposes" under the California Consumer Privacy Act (CCPA). We do not sell your personal information for the intents and purposes of CCPA. We may disclose personal data to third parties or allow them to collect personal data from our Services as described above, if those third parties are authorized Service Providers or business partners who have agreed to our contractual limitations as to their retention, use, and disclosure of such personal data, or if you integrate the services of third parties with our Services, or direct us to disclose your personal data to third parties.

10. Who is responsible for your data?

Certain data protection laws and regulations, such as the EU and UK GDPR, typically distinguish between two main roles for parties processing personal data: the "**Data Controller**", who determines the purposes and means for processing; and the "**Data Processor**", who processes the data on behalf of the Data Controller.

Connecteam is typically the Data Controller of its Candidates' personal data, and with respect to which, assumes the responsibilities of a Data Controller (solely to the extent applicable under the law), and as set forth in this Notice. In such instances, our Service Providers processing such data will assume the role of Data Processors.

11. Will this Notice be updated?

We may update this notice to reflect changes in our privacy practices. If we make any changes that we deem as "material", we will update this page prior to the change becoming effective.

12. What if you have questions?

DPO: We have appointed a data protection officer (DPO) who is responsible for overseeing our privacy practices. If you have any comments or questions about this Privacy Notice, or if you wish to exercise any of your legal rights as set out herein, please contact using the details set out below:

Name of DPO: Advocate Chen Shofar
Email address: dpo@connecteam.com

EU and UK Representatives: Maetzler Rechtsanwalts GmbH & Co KG (Prighter) has been designated as Connecteam's representative in the European Union for data protection matters pursuant to Article 27 of the GDPR. Maetzler Rechtsanwalts GmbH & Co KG may be contacted only on matters related to the processing of Personal Data in the EU. To make such an inquiry, please contact Maetzler Rechtsanwalts GmbH & Co KG through this contact form: https://prighter.com/q/14267474.

Prighter Ltd. has been designated as Connecteam's representative in the United Kingdom for data protection matters pursuant to Article 27 of the UK-GDPR. Prighter Ltd. may be contacted only on matters related to the processing of Personal Data in the UK. To make such an inquiry, please contact Prighter Ltd. through this contact form: https://prighter.com/q/14267474

If you have any comments or questions regarding our data practices or your privacy, or if you have any concerns regarding your personal data held with us, or if you wish to make a complaint about how your personal data is being processed by Connecteam please contact our DPO at dpo@connecteam.com.