Date: 23rd December, 2022

To,
Nawksoft Solutions Private Limited
Row House No. 11,
Eastern Paradise, S. No. 124/1,
Baner Road, Baner, Pune - 411 021
Maharashtra, India

Dear Sir/Madam,

Ref: Legal Opinion on queries pertaining to operation of a business engaged in providing commitment intelligence for candidates, through its SAAS platform.

We have perused your query as regards the legal implications of an online recruiter's network business in India under the applicable laws. We understand that the factual background in the instant case is as under:

A. FACTS:

1. Nawksoft Solutions Private Limited ("**NSPL**") is a company established in India, having its registered office in Pune, Maharashtra.

2. As per its Memorandum of Association, the main objects of NSPL *inter alia* includes: (b) to carry on the business of developing technologies using artificial intelligence, software designing, development, customisation, implementation, maintenance, testing and benchmarking, designing, developing and dealing in computer software and solutions, and to import, export, sell, purchase, distribute, services to assist entrepreneurs, other business to increase efficiency and help to reduce the cost in India and abroad; (c) to carry on the business of software development and computer designing, job works, customization and also to provide technical services, training, consultancy related to hardware and software, information technology, to undertake computer related jobs as internet, communication network, e-commerce, web hosting, maintenance of web sites, web site designing, development of portals, multimedia and to carry on all kinds of business in India or abroad related to information and technology, computer related assignments WAP application development, franchising;.

3. In line with its main objects, NSPL is *inter alia* engaged in the business of providing commitment intelligence for candidates, through its SAAS platform under the name '**OpenOffers**' ("**Online SaaS Platform**").

4. At present, NSPL intends to create a database of all the candidates who have accepted an offer from any corporate entities/ recruitment agencies **("Client/s")** and the same is accessible to all the Clients who have subscribed to the Online SaaS Platform.

5. The Clients are required to sign-up and subscribe to the Online SaaS Platform by submitting certain data with regard to its organization. In the event any individual is signing up on the Online SaaS Platform, his/her personal information such as name, corporate email address and contact number would also form a part of such data. Post submission of the details, the Client is required to accept the sign up proposal form and execute the SaaS Agreement pursuant to which the Client would be successfully registered as a subscriber on the Online SaaS Platform.

6. Pursuant to successful subscription as above, the Clients would share the following details of their respective candidates who have accepted job offer: (i) PAN number (ii) Name; (iii) Email address; (iv) Contact number; (v) Offer acceptance date; and (vi) Proposed date of joining. In the event the Client is a recruitment agency, such a Client would be additionally required to submit the the email address of the client of the recruitment agency;

7. NSPL would store certain information of the candidates on its Online SaaS Platform such as the PAN number which serves as an unique identification number of the candidate in one-way-hash format (i.e. not disclosing all the characters, by displaying # or similar signs in places to mask complete identification), offer acceptance date, and committed date of joining. As mentioned to us, a one-way-hash is a mathematical function that generates a unique fingerprint of the input data and there is no way to get back to the original input data. Thereby ensuring that the Online SaaS Platform does not store the data such as PAN number and it will be infeasible for the Online SaaS Platform to obtain the PAN Card number of the candidate from the one-way-hash.

8. In the event the PAN number of the candidate is not available, NSPL would accept and store his/her name, email address and contact number. Additionally, the Online SaaS Platform would compute a commitment score of the candidates based on their behavioural pattern such as the numbers of offers the candidate backed out from, the number of offers ghosted or rejected by the candidate and instances of abscondment by the candidate in any previous organization **("Commitment Score")**.

9. The Clients registered on the Online SaaS Platform would be able to access the above specified information via their account on the Online SaaS Platform. However, the Online SaaS Platform does not specify the names of the companies from which the candidate has received offers and the same is kept anonymous. A database of the company/ recruitment agencies is created at the back-end as they are the subscribers to the Online SaaS Platforms.

10. NSPL stores the PAN card details of the candidates in a one-way-hash format and does not store the PAN card details in plain text on its system. NSPL does not sell/ transfer the data to

any other third party and all the data or information shared via the Online SaaS Platform remains with NSPL.

11. NSPL intends to assess whether the receiving, storage and display of information on the Online SaaS Platform in the manner as specified above is legally permissible under the applicable laws in India and under GDPR regulations and the implications thereunder.

12. NSPL has empanelled a vendor to establish policies, procedures, systems to ensure the compliance to GDPR, ISO27001, and SOC2. NSPL is currently undergoing the process of getting compliant on these norms.

B. QUERIES:

Considering the above factual background, you have sought our opinion of the following queries:

1. Whether NSPL would be legally permitted to receive, store and display the candidate information received from the Client, in accordance with the applicable laws in India?

2. What compliances does NSPL need to adhere to, in order to ensure compliance under the applicable laws in India?

3. Whether the receiving, storage and display of the candidate information by NSPL in permissible under the General Data Protection Regulations (GDPR)? If yes, what are the compliances that NSPL needs to adhere to?

C. RELEVANT LAWS AND REGULATIONS:

1. The Information Technology Act, 2000 **("IT Act")** and the rules thereunder
2. Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011 **("IT Rules 2011)**
3. General Data Protection Regulations **("GDPR")**

D. RESPONSE TO THE QUERIES AND ANALYSIS:

1. RESPONSE TO QUERY NO. 1:

a. The IT Act read with the rules thereunder regulates the collection, disclosure, storage, processing, etc. of information received from any individual within India.

b. The IT Rules 2011 specifically deals with collection, storage and disclosure of information or personal information or data of any individual.

c. **Receipt of Candidate Information**

(1) Rules 6(1) of the IT Rules 2011 reads as follows: "*Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation*."

(2) Further rule 7 of the IT Rules 2011 states that, "*A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer*."

(3) Thus, the bare reading of the rules specified above state that the Client is obligated to obtain consent from its candidates prior to disclosing the information of the candidates to NSPL. If such consent is legally obtained, in our view, there are no obligations imposed on the third party receiving information i.e. NSPL to obtain consent from any individual prior to receiving such information.

(4) Further, there is no explicit prohibition under any applicable laws in India including the IT Act and the IT Rules 2011 with regard to receiving information from any body corporate.

(5) Thus, we are of the opinion that NSPL is permitted legally under the Indian laws to receive candidate information from the Clients subject to compliances under IT Act and rules thereunder (refer to response to query 2 below).

(6) However, as per rule 6 (1) and rule 7 of the IT Rules 2011, the information related to any individual may be shared with any third party only in the event the individual whose information is being disclosed to the third party has consented to such a disclosure under a lawful contract. Thus, in the present case, the Client needs to obtain a prior written consent from the candidates prior to sharing the information with NSPL. We would like to add, it would be prudent to ensure that the consent is expressly and explicitly set out and provided for where there could be no scope of negative interpretation of such consent.

(7) As stated above even in the absence of any direct obligation on NSPL to obtain consent from the candidates with regard to receiving and storage of their information, we recommend that NSPL safeguards itself against any liability arising on account of failure of the Client to obtain consent from its candidates.

(8) We recommend that NSPL obtains a specific indemnity from the Client safeguarding itself against any claims, legal proceedings or legal action which may arise on account of failure of

the Client to obtain consent from its candidates or any unauthorised disclosure of information by the Client. This may be included under the service agreement executed between NSPL and the Client or the parties choose to execute a separate indemnity bond in this regard. Secondly, a provision stating that the Client is sharing the candidate information by legal means, which is necessary for compliance of the legal obligation and after obtaining consent from the relevant candidate should be included under the privacy policy of NSPL displayed on the Online SaaS Platform. The said privacy policy also needs to specifically include the mannerism in which the disclosed candidate information would be used by NSPL (refer to query 2 below for a detailed explanation on the compliances with regard to the privacy policy).

d. **Storage of Candidate Information**

(1) Similarly, in our view, with regard to storage of the information, there is no explicit prohibition under any applicable laws in India including the IT Act and the IT Rules 2011 with regard to storage of the information received from any body corporate. However, it is important to note that as per rule 7 of the IT Rules 2011, the recipient third party i.e. NSPL is required to comply with the same level of data protection that is adhered to by the body corporate as provided for under the said rules (refer to response to query 2 below).

e. **Display of Candidate Information on the Online SaaS Platform**

(1) With regard to the display of the candidate information on the Online SaaS Platform, we understand that the Company shall, upon input of a candidate's information from a Client, display the following information on the Online SaaS Platform: (i) Name, contact number and/ or email address of the candidate as provided by the Client; (iii) Commitment Signals viz. offer accepted, recommitted, renegotiating, joined, backed-out, ghosted, absconded, BGV Started and (ii) Commitment Score (collectively referred to as **"Candidate Information")**.

(2) Rule 6(4) of the IT Rules 2011 states that, "*The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further.*" Thus, there is an explicit prohibition under the rules with regard to further ***disclosure of the sensitive personal data or information*** by the recipient third party. Accordingly, NSPL is not legally permitted to display such information on the Online SaaS Platform which is not available with a Client.

For example:
Client - Enterprise A: has only name and contact number of the candidate say Mr. XYZ and is presumed not to have any other information of this candidate.

Client – Enterprise B: has the name, email ID, contact number and PAN of Mr. XYZ.

So, upon input of just the name of XYZ on the Online SaaS Platform by Enterprise A, the Online SaaS Platform should not display any other information of XYZ which Enterprise does not hold.

Clients get to see only the identification information that they have provided for a candidate, and not the information received from other clients on the Online SaaS Platform for the same candidate.

(3) Rule 2 (1) (i) of the IT Rules 2011 defines Personal information as "*any information that relates to a natural person which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person*". Section 2 (1) (v) of the IT Act defines information as "*data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche*". Further, rule 3 of the IT Rules 2011 reads as follows: *"Sensitive personal data or information of a person means such personal information which consists of information relating to;--(i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise*."

(4) It must be noted that rule 6(4) prohibits further disclosure of any sensitive personal information and data. The rule 3 of IT Rules 2011 specifies an exhaustive list of information which would be classified as sensitive personal information. We observe that name, contact number, email address or PAN of an individual has not been classified as sensitive personal information or data under the IT Rules 2011. Thus, we are of the view that the Candidate Information proposed to be displayed by NSPL on the Online SaaS Platform does not fall under the definition of sensitive personal information and data.

(5) However, with a view to ensure that the Candidate Information does not even fall under the category of "Personal information" as defined under the IT Rules 2011, we recommend that the Candidate Information should be displayed in such a manner so as to ensure that the said information or in combination with other information, is not capable identifying the candidate. For instance, all the Candidate Information such as the name, contact number, email address should be displayed in a similar hash format as the PAN (E.g. Name: Vi***a Gh****s).

(6) Accordingly, we are of the view that NSPL may display the Candidate Information on the Online SaaS Platform in the manner as specified above and subject to fulfilling the compliances specified under IT Act and its Rules thereunder *(refer to response to query 2 below)*.

f. In the above circumstances and background, we are of the view that NSPL is legally permitted as per the applicable laws in India to receive, store and display the Candidate Information

only in the manner as specified above and subject to compliance as mentioned herein, for which NSPL would be taking due care to abide by all the compliances.

2. RESPONSE TO QUERY NO. 2:

a. The IT rules 2011 specifies certain compliances which body corporate needs to adhere to while receiving, storing or dealing with information of any individual. We understand that NSPL would not be directly collecting the Candidate Information but would be receiving the same from the Clients. However, NSPL is required to comply with certain obligations specified under the IT Rules 2011.

b. Rule 4 of the IT Rules 2011 reads as follows: "The body corporate or any person who on behalf of body corporate collects, receives, posses, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for- (i) clear and easily accessible statements of its practices and policies; (ii) type of personal or sensitive personal data or information collected under rule 3; (iii) purpose of collection and usage of such information; (iv) disclosure of information including sensitive personal data or information as provided in rule 6; (v) reasonable security practices and procedures as provided under rule 8.

c. Thus, since NSPL would be handling certain information provided by the Clients including but not limited to the Candidate Information, NSPL needs to adopt a comprehensive privacy policy in accordance with Rule 4 of the IT Rules 2011. Further, as specified above in response to query 1 above, the privacy policy needs to include a provision stating that the Client is sharing the candidate information by legal means and after obtaining consent from the relevant candidate.

d. Rule 7 of the IT Rules 2011 states that a body corporate may transfer sensitive personal data or information including any information, to any other body corporate that ensures the same level of data protection that is adhered to by the body corporate as provided for under the IT Rules 2011. Thus, NSPL needs to adopt for comprehensive and robust data protection in the manner as may be applicable to the Client under the IT Act and the rules thereunder.

e. Rule 8 of the IT Rules 2011 specifies certain standard security practices and procedures which are to be adopted by any body corporate dealing with information of individuals. Rule 8 of the IT Rules 2011 states that an entity needs to implement such security practices and standards such as the international Standard IS/ISO/IEC 27001 on "Information Technology -Security Techniques - Information Security Management System - Requirements". Further, the entity needs to have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being

protected with the nature of business. Further, in the event of an information security breach, the entity shall be required to demonstrate, as and when called upon to do so by the agency mandated/under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

f. Further, the entity adopting the security standards such as the IS/ISO/IEC 27001 standard shall be deemed to have complied with reasonable security practices and procedures provided that such standard have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

g. Thus, based on the understanding of the nature of the business operation of NSPL, we are of the view that it needs to fulfil and abide with the above mentioned compliances in accordance with the IT Act and IT Rules 2011 for which we are informed that NSPL is currently doing the needful.

3. RESPONSE TO QUERY NO. 3:

a. **Applicability of GDPR**

(1) The GDPR deals with processing of personal data of subject matter based out of the European Union region and rules relating to the free movement of personal data. The GDPR imposes certain obligations on the controller as well as the processor of the personal data.

(2) In the event the Client and the candidates of the Client are based out of the European Union, NSPL would be processing personal data of the individuals based out of the European Union and thus would be required to comply with the GDPR.

(3) The term "controller" has been defined under Article 4(7) of the GDPR as "*the natural or **legal person**, public authority, agency or other body **which, alone or jointly with others, determines the purposes and means of the processing of personal data**; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*"

(4) The term "personal data" has been defined under Article 4(1) of the GDPR as follows: "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*."

(5) The term "processing" has been defined under Article 4(2) of the GDPR as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*."

(6) Based on the bare reading of the definitions specified above it is clear that the Candidate Information would fall under the scope of the term "personal data" and the collection, recording, storage, etc. of the Candidate Information would be considered as "processing" under GDPR.

(7) The definition of the term "controller" includes any legal person who determines the means and purpose of processing of the personal data. We understand that NSPL would be processing the Candidate Information in such a manner and for such purpose as it may solely determine. Thus, we are of the view that NSPL falls under the definition of a controller under the GDPR.

b. **Compliances under GDPR**

(1) NSPL would thus be required to comply with all the regulations applicable to a controller under the GDPR. Article 24 of the GDPR deals with the responsibilities of a controller in addition to the other obligations specified under the GDPR. The controller is, *inter alia,* required to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR (refer to article 32 of the GDPR). The said measures shall be reviewed and updated where necessary. Article 25 further states that the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. The obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

(2) Further, where proportionate in relation to processing activities, the controller shall ensure implementation of appropriate data protection policies. The controller also needs to adhere to the approved code of conduct specified under Article 40 of the GDPR or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

(3) Article 30 states that the controller shall maintain a record of processing activities under its responsibility in the manner as specified under the said article. A controller is also required to designate a data protection officer in the manner as specified under Article 37 of the GDPR.

(4) Further, a controller is required to adopt a privacy policy in accordance with Article 12 of the GDPR. Thus, NSPL is required to ensure that the privacy policy adopted by it is in compliance with the IT Act as well as the GDPR.

(5) Please note that the above mentioned provisions are not exhaustive and NSPL is required to comply with all the provisions applicable to a controller under GDPR including but not limited to the provisions listed above.

(6) We recommend that since the Client would also fall under the definition of a "controller" under the GDPR, NSPL should obtain a specific indemnity from the Client safeguarding against any claims, legal proceedings or legal action which may arise on account of breach by the Client of the GDPR. This may be included under the service agreement executed between NSPL and the Client or the parties may execute a separate indemnity bond in this regard. Secondly, a provision stating that the Client is sharing the candidate information in accordance with the GDPR should be included under the privacy policy of NSPL displayed on the Online SaaS Platform.

c. Based on the facts and analysis specified above, we are of the opinion that NSPL is required to comply with the GDPR in addition to the applicable Indian legislations, for which we are informed that NSPL is currently doing the needful.

We trust the above sufficiently meets your queries. Should you require any further clarifications on the same, please do not hesitate to contact us.

Yours faithfully,

NR Chhaporia

Partner
ANB Legal, Advocates & Solicitors

Disclaimers:

The opinions set out above are subject to the following assumptions/qualifications:
i. This legal opinion is confined to and given on the basis of the applicable laws of India as at the date hereof, and we do not express any opinion on the laws of any other jurisdiction. We assume no obligation to update this legal opinion on any events subsequent to its issue.
ii. All signatures, stamps and seals on the documents submitted to us are assumed, without independent verification, to be genuine and in conformity to the original documents.
iii. As to the other matters of fact that are material to the opinions expressed herein, we have not conducted any independent verification and have relied on the information provided by NSPL . We have no reason to believe that the same are not correct and genuine.
iv. This legal opinion is addressed to NSPL , in connection with proposed transactions as mentioned herein above. It may not be relied upon for any other purpose.
v. Our views are not binding on any authority or court, and hence, no assurance is given that a position contrary to the opinions expressed herein, will not be asserted by any statutory authority and/or sustained by

an appellate authority or a court of law. The management of NSPL acknowledges and accepts full responsibility for all decisions taken by them in this regard.

******