Data Subject Access Request Policy

1. **Introduction**

    1. The Company holds personal data (or information) about job applicants, employees, clients, customers, suppliers, business contacts and other individuals for a variety of business purposes.

    2. Under the General Data Protection Regulation (GDPR), individuals (known as 'data subjects') have a general right to find out whether we hold or process personal data about them, to access that data. This is known as the right of access, or the right to make a data subject access request. The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that we are undertaking.

    3. Our GDPR Committee is responsible for ensuring:

        1. that all data subject access requests are dealt with in accordance with the GDPR and other relevant legislation and guidance; and
        2. that all staff have an understanding of the GDPR and other relevant legislation and guidance in relation to data subject access requests and their personal responsibilities in complying with the relevant aspects of the GDPR and other relevant legislation and guidance.

    4. This policy provides guidance for staff members on how data subject access requests should be handled, and is intended for internal use. It is not a privacy policy or statement, and is not to be made routinely available to third parties.

    5. This policy applies to all staff but much of it is aimed primarily at those members of staff who are authorised to handle data subject access requests. These sections are identified by the words '(authorised staff)' appearing in the section title. For other staff members, it provides guidance on:

        1. what to do if you receive a data subject access request (see paragraph 3 below); and
        2. how to decide whether a request for information is a data subject access request (see paragraph 2 below).

    6. Failure to comply with the right of access under the GDPR puts both staff and the Company at potentially significant risk, and so the Company takes compliance with this policy very seriously. For further information on the consequences of failure to comply, see paragraph 15 below.

    7. We will review and update this policy in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

    8. If you have any questions regarding this policy, please contact **any member of the GDPR Committee**.

2. **How to recognise a data subject access request (all staff)**

    1. A data subject access request is a request from an individual (or from someone acting with the authority of an individual):

        1. for confirmation as to whether we process personal data about him or her and, if so
        2. for access to that personal data
        3. and certain other supplementary information

    2. Such a request should be made in writing. For example, a letter which states 'please provide me with a copy of all the information that you have about me' will be a data subject access request and should be treated as such.

    3. All data subject access requests should be immediately directed to compliance@ineedleads.co.uk in accordance with paragraph 3 below.

3. **What to do when you receive a data subject access request (all staff)**

    1. A subject access request can either be made directly from the link provided within the corporate Privacy policy/notice. Or on occasion staff may receive a request directly from the data subject by any communication method. Below is the process when a direct request is received by staff.

    2. If you receive a data subject access request and you are not authorised to handle it, you must immediately take the steps set out in paragraphs 3.3 (request received by email) or 3.4 (request received by letter) There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

    3. For information on what amounts to a data subject access request, see paragraph 2 above. If you are in any way unsure as to whether a request for information is a data subject access request, please contact **any member of the GDPR Committee**

    4. If you receive a data subject access request by email, you must immediately forward the request to this email address: compliance@ineedleads.co.uk

    5. If you receive a data subject access request by letter you must send a scanned copy of the letter to this email address compliance@ineedleads.co.uk

    6. You will receive confirmation when the request has been received. If you do not receive such confirmation within [two] working days of sending it, you should compliance@ineedleads.co.uk to confirm safe receipt.

    7. You must not take any other action in relation to the data subject access request. The EU-Privacy mailbox is operational and will keep you advised (in writing) of what action should be taken and when.

4. **Conditions for responding to a valid request (authorised staff)**

    1. Where we process a large quantity of information about an individual, we may need to ask the individual to specify the information or processing activities to which the request relates.

2. We will not usually charge a fee for responding to a data subject access request. We may, however, charge a reasonable fee (based on the administrative cost of providing the information) for responding to a request:

    1. that is manifestly unfounded or excessive, e.g. repetitive; or
    2. for further copies of the same information.

5. **Identifying the data subject (authorised staff)**

    1. Before responding to a data subject access request, we will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward.

    2. We will not retain personal data, e.g. relating to former employees for the sole purpose of being able to react to potential data subject access requests in the future.

    3. If we have doubts as to the identity of the person making the data subject access request, we may ask for additional information to confirm his or her identity. Typically we will request a copy of the individual's driving license or passport to enable us to establish his or her identity and signature (which should be compared to the signature on the data subject access request and any signature we already hold for the individual). We also ask for a recent utility bill (or equivalent) to verify the individual's identity and address.

    4. If, having requested additional information, we are still not in a position to identify the data subject, we may refuse to act on a data subject access request (see paragraph 7 below).

6. **Refusing to respond to a request (authorised staff)**

    1. We may refuse to act on a data subject access request where:

        1. even after requesting additional information in accordance with paragraph 5.2, we are not in a position to identify the individual making the data subject access request;

        2. requests from an individual are manifestly unfounded or excessive, e.g. because of their repetitive character or, in certain circumstances, where the request relates to large amounts of data.

    2. If we intend to refuse to act on a data subject access request, we will inform the individual no later than one month after receiving his or her request:

        1. of the reason(s) why we are not taking action; and
        2. that they have the right to complain to the Data Protection regulatory body and seek a judicial remedy.

7. **Time limit for responding to a request (authorised staff)**

    1. Once a data subject access request is received, the Company must provide the information requested without delay and at the latest within one month of receiving the request. You should therefore make a note of when request was received and when the time limit will end.

2. If a data subject access request is complex or the data subject has made numerous requests, the Company:

    1. may extend the period of compliance by a further two months; and
    2. must inform the individual of the extension within one month of the receipt of the request, and explain why the extension is necessary.

8. **Information to be provided in response to a request (authorised staff only)**

    1. The individual is entitled to receive access to the personal data we process about him or her and the following information:

        1. the purposes for which we process the data;
        2. the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
        3. where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
        4. the fact that the individual has the right:
            1. to request that the Company rectifies, erases or restricts the processing of his personal data; or
            2. to object to its processing;
            3. to lodge a complaint with the Data Protection regulatory body
        5. where the personal data has not been collected from the individual, any information available regarding the source of the data;
        6. any automated decision we have taken about him or her (see paragraph 9 below), together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

    2. The information referred to in paragraph 8.1 should be provided using the Company's standard form response to data subject request—right of access:

        1. in a way that is concise, transparent, easy to understand and easy to access;
        2. using clear and plain language, with any technical terms, abbreviations or codes explained;
        3. in a commonly-used electronic format, if the data subject access request was made electronically, unless otherwise requested by the individual;

9. **Automated decision-making**

    1. If the data subject access request specifically asks for information about the logic behind any automated decision that we have taken in relation to important matters relating to the individual (e.g. performance at work, creditworthiness, reliability or conduct), we must provide a description of the logic involved in that automated decision, subject to the following conditions:

        1. the automated decision must have constituted the sole basis for the decision;;
        2. in providing a description of the logic we are not required to reveal any information which constitutes a trade secret (e.g. the algorithm behind a credit scoring system).

    2. If the Company carries out automated decision-making in relation to an individual, the data subject access request may include a request:

        1. for information relating to the automated decision;

2. for human intervention on the part of the Company, i.e. to ask that an individual with the authority and competence to change the decision should review the automated decision, considering all the available data;
3. to express his or her point of view on the automated decision; and/or
4. to contest the automated decision.

10. If such a request is received, **the GDPR Committee** will ensure that it is dealt with in accordance with the GDPR and other relevant legislation and guidance.

11. **How to locate information (authorised staff only)**

    1. The personal data we need to provide in response to a data subject access request may be located in several of our electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

    2. Depending on the type of information requested, you may need to search all or some of the following:

        1. electronic systems, e.g. databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
        2. manual filing systems in which personal data are accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data;
        3. data systems held externally by our data processors, e.g. external payroll service providers;
        4. occupational health records;
        5. pensions data held by *pension provider/administrator*;
        6. share scheme information held by *share scheme administrator*
        7. insurance benefit information held by *benefit provider*
        8. data held by external support, consultants etc

    3. You should search these systems using the individual's name, employee number, customer account number or other personal identifier as a search determinant.

12. **What is personal data? (authorised staff)**

    1. Once we have carried out the search and gathered the results, we will need to select the information to be supplied in response to the data subject access request. The individual is only entitled to receive information which constitutes his or her personal data.

    2. Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, e.g. their name, identification number, location data or online identifier. It may also include personal data that has been pseudonymised (e.g. key-coded), depending on how difficult it is to attribute the pseudonym to a particular individual.

13. **Requests made by third parties on behalf of the individual (authorised staff only)**

    Occasionally we may receive a request for data subject access by a third party (an 'agent') acting on behalf of an individual. These agents may include parents, guardians, legal representatives and those acting under a power of attorney or other legal authority. The agent must provide sufficient evidence that he or she is authorised to act on behalf of the individuals.

14. **Exemptions to the right of subject access (authorised staff only)**

1. In certain circumstances we may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

2. **Crime detection and prevention**: We do not have to disclose any personal data which we are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. We are still required to provide as much of the personal data as we able to. For example, if the disclosure of the personal data could alert the individual to the fact that he or she is being investigated for an illegal activity (i.e. by us or by the police) then we do not have to disclose the data since the disclosure would be likely to prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

3. **Protection of rights of others**: We do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information (or that information and any other information that we reasonably believe the data subject is likely to possess or obtain), unless:

    1. that other individual has consented to the disclosure of the information to the individual making the request; or
    2. it is reasonable to disclose the information to the individual making the request without the other individual's consent, having regard to:
        1. the type of information that would be disclosed;
        2. any duty of confidentiality owed to the other individual;
        3. any steps taken by the controller with a view to seeking the consent of the other individual;
        4. whether the other individual is capable of giving consent; and
        5. any express refusal of consent by the other individual.

4. **Confidential references**: We do not have to disclose any confidential references that we have given to third parties for the purpose of actual or prospective:

    1. education, training or employment of the individual;
    2. appointment of the individual to any office; or
    3. provision by the individual of any service

5. This exemption does not apply to confidential references that we receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means you must consider the rules regarding disclosure of third-party data set out in paragraph 12 before disclosing the reference.

6. **Legal professional privilege**: We do not have to disclose any personal data which are subject to legal professional privilege. There are two types of legal professional privilege:

    1. 'Advice privilege' covers confidential communications between the Company and our lawyers where the dominant purpose of the communication is the seeking or giving of legal advice;
    2. 'Litigation privilege' covers any document which was created with the dominant purpose of being used in actual or anticipated litigation (e.g. legal proceedings before a court or tribunal). Once a bona fide claim to litigation privilege ends, the documents in the file which were subject to

litigation privilege become available if a data subject access request is received.

7. **Corporate finance**: We do not have to disclose any personal data which we process for the purposes of, or in connection with, a corporate finance service if:

    1. disclosing the personal data would be likely to affect the price of an instrument; or
    2. disclosing the personal data would have a prejudicial effect on the orderly functioning of financial markets or the efficient allocation of capital within the economy and we believe that it could affect a person's decision:

        1. whether to deal in, subscribe for or issue an instrument;
        2. whether to act in a way likely to have an effect on a business activity, e.g. on the industrial strategy of a person, the capital structure of an undertaking or the legal or beneficial ownership of a business or asset; and]

8. **Management forecasting**: We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity. Examples of management forecasting and planning activities include staff relocations, redundancies, succession planning, promotions and demotions. This exemption must be considered on a case-by-case basis and must only be applied to the extent to which disclosing the personal data would be likely to prejudice the conduct of that business or activity.

15. **Deleting personal data in the normal course of business (authorised staff only)**

1. The information that we are required to supply in response to a data subject access request must be supplied by reference to the data in question at the time the request was received. However, as we have one month in which to respond and we are generally unlikely to respond on the same day as we receive the request, we are allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data are supplied if such amendment or deletion would have been made regardless of the receipt of the data subject access request.

2. We are, therefore, allowed to carry out regular housekeeping activities even if this means that we delete or amend personal data after the receipt of a data subject access request. What we are not allowed to do is amend or delete data because we do not want to supply the data.

16. **Consequences of failing to comply with this policy (all staff)**

1. If we fail to comply with a subject access request, or fail to provide access to all the personal data requested, or fail to respond within the one-month time period, we will be in breach of GDPR and other relevant legislation. This may have several consequences:

2. The Company takes compliance with this policy very seriously. If we fail to comply with a subject access request, or fail to provide access to all the personal data requested, or fail to respond within the one-month time period, we will be in breach of GDPR and other relevant legislation. This may have several consequences:

    1. it may put at risk the individual(s) whose personal information is being processed;

2. the individual may complain to the Data Protection regulatory body and this may lead the Data Protection regulatory body to investigate the complaint. If we are found to be in breach, enforcement action could follow, which carries the risk of significant civil and criminal sanctions for the Company and, in some circumstances, for the individual responsible for the breach;
3. if an individual has suffered damage, or damage and distress, as a result of our breach of the GDPR or other relevant legislation, he or she may take us to court and claim damages from us; and
4. a court may order us to comply with the subject access request if we are found not to have complied with our obligations under the GDPR and other relevant legislation.

3. Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

17. **Contacts and responsibilities (all staff)**

1. This Policy will be reviewed annually by the GDPR Committee.
2. Any questions regarding this Policy should be addressed to any member of the GDPR Committee.