Gi GROUP UK POLICY

DATA PROTECTION POLICY

THE PURPOSE OF THIS POLICY

All organisations that process personal data are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their personal data whilst imposing certain obligations on the organisations that process their data.

As a HR services company involved in recruitment, coaching, mentoring, career development, outplacement, training and other HR services Gi Group companies collect and process both personal data and sensitive personal data. It is required to do so to comply with other legislation, or where it is in the Company's legitimate interests to do so. It is also required to keep this data for different period of time depending on the nature of the data.

This policy applies to all of the Company's staff including employees, workers, contractors, agency workers, consultants and directors who process personal data.

This policy sets out what the Company expects from its staff in order for the Company to comply with applicable law. All staff must read, understand and comply with this policy and attend training on its requirements as necessary. Any breach of this policy may result in disciplinary action.

DEFINITIONS

In this policy, the following terms have the following meanings:

'Company'	means all Gi Group companies, including Gi Group, INTOO and TACK
'GDPR'	means General Data Protection Regulations
'Consent'	means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
'Data Controller'	means an individual or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data
'Data Processor'	means an individual or organisation that processes personal data on behalf of the data controller
'Personal Data'	means any information relating to an individual who can be identified, such as by 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 an individual
'Personal Data Breach'	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
'Processing'	means any operation or set of operations performed on personal data, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
'Profiling'	means any form of manual or automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual; in particular, to analyse or predict aspects concerning an individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
'Anonymisation'	means the processing of personal data in such a manner that the personal data can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;
'Sensitive Personal Data'	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, biometric data, data concerning health, an individual's sex life or sexual orientation or an individual's criminal convictions. For the purposes of this policy the term **'Personal Data'** includes **'Sensitive Personal Data'** except where we specifically need to refer to Sensitive Personal Data.
'Supervisory Authority'	means an independent public authority that is responsible for monitoring the application of data protection. In the UK, the supervisory authority is the Information Commissioner's Office (ICO).

The Company processes personal data in relation to its candidates, workers, employees and customer contacts and is a data controller for the purposes of the Data Protection Laws. Gi

Group, TACK and INTOO are registered with the ICO and their registration numbers are
Z5917046 (Gi Group Recruitment Limited)
Z8816295 (TACK)
ZA369900 (INTOO (UK) Limited
.

REASONS FOR PROCESSING

The Company may hold personal data on individuals for the following purposes:

a) run recruitment and promotion processes;
b) maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
c) operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
d) operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
e) operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
f) obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
g) operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
h) ensure effective general HR and business administration;
i) provide references on request for current or former employees;
j) respond to and defend against legal claims; and
k) maintain and promote equality in the workplace
l) provide services such as training, career development, coaching, mentoring or outplacement to you
m) inform you of latest products, services or events offered by the Group
n) create and maintain accurate business records for business purposes such as invoicing

1. THE DATA PROTECTION PRINCIPLES

The Data Protection Laws require the Company acting as either Data Controller or Data Processor to process data in accordance with the principles of the GDPR. These require that personal data is:

a) Processed lawfully, fairly and in a transparent manner;
b) Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept for no longer than is necessary for the purposes for which the personal data is processed;
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and that
g) The Data Controller shall be responsible for, and be able to demonstrate, compliance with the principles.

2. LEGAL BASIS FOR PROCESSING

The Company will only process personal data where it has a legal basis for doing so. Legal bases are listed in sections 17 and 18. Where the Company does not have a legal basis for processing personal data any processing will be a breach of the Data Protection Laws.

The Company will review the personal data it holds on a regular basis to ensure it is being lawfully processed and is accurate, relevant and up to date.

The Company will ensure that personal data is kept for no longer than is necessary for the purposes for which the personal data is processed, and in accordance with the Company's Data Retention Policy.

Before transferring personal data to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support), the Company will establish that it has a legitimate reason for making the transfer.

Legitimate reasons are listed in section 1.

3. PRIVACY BY DESIGN AND BY DEFAULT

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all processing activities. This includes implementing measures such as:

a) data minimisation (i.e. not keeping data for longer than is necessary);
b) anonymization
c) cyber security
d) education and training
e) non-disclosure agreements

4. PRIVACY NOTICES

Where the Company collects personal data from the individual or collects personal data other than from the individual directly, the Company will ensure that their privacy notice is easily accessible at all times. This may be via the Company's Internet or Intranet services.

Where the Company intends to further process the personal data for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further processing.

5. SUBJECT ACCESS REQUESTS

The individual is entitled to access their personal data on request from the Data Controller. A copy of the form is available on our websites or can be requested by emailing uk.privacy@gigroup.com

6. RECTIFICATION

The individual has the right to ask the Company to rectify any inaccurate or incomplete personal data concerning the individual.

If the Company has given the personal data to any third parties, it will tell those third parties that it has received a request to rectify the personal data unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however, the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

7. ERASURE

The individual has the right to ask the Company to erase their individual personal data in certain circumstances.

If the Company receives a request to erase it will ask the individual if they want their personal data to be removed entirely or whether they are happy for their details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). The Company cannot keep a record of individuals whose data it has erased so the individual may be contacted again by the Company should the Company come into possession of the individual's personal data at a later date.

If the Company has made the data public, it shall take reasonable steps to inform other data controllers and data processors processing the personal data about the request to erase the personal data, taking into account available technology and the cost of implementation.

If the Company has given the personal data to any third parties, it will tell those third parties that it has received a request to erase the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however, the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

The Data Controller is not obliged to erase an individual's data where it would be in breach of the Companies legal obligations.

8. RESTRICTION OF PROCESSING

The individual has the right to ask the Company to restrict its processing of their individual personal data where:

a) The individual challenges the accuracy of the personal data;
b) The processing is unlawful and the individual opposes its erasure;
c) The Company no longer needs the personal data for the purposes of the processing, but the personal data is required for the establishment, exercise or defence of legal claims; or
d) The individual has objected to processing (on the grounds of a public interest or legitimate interest) pending the verification of whether the legitimate interests of the Company override those of the individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to restrict the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

9. DATA PORTABILITY

The individual shall have the right to receive personal data concerning them, which they have provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit the data to another data controller in circumstances where:

a) The processing is based on the individual's consent or a contract; and
b) The processing is carried out by automated means.

Where feasible, the Company will send the personal data to a named third party on the individual's request.

10. OBJECT TO PROCESSING

The individual has the right to object to their personal data being processed based on a public interest or a legitimate interest. The individual will also be able to object to the profiling of their data based on a public interest or a legitimate interest.

The Company shall cease processing unless it has compelling legitimate grounds to continue to process the personal data which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their personal data for direct marketing. Any marketing communication sent by the Group contains required opt-out links enabling individuals to unsubscribe or to update their personal preferences.

11. ENFORCEMENT OF RIGHTS

All requests regarding individual rights should be sent to the **Mr. Gabriele Faggioli** uk.privacy@gigroup.com

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability, objection, automated decision making processes or profiling within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

12. AUTOMATED DECISION MAKING

The Company will not subject individuals to decisions based on automated processing that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

Is necessary for the entering into or performance of a contract between the data controller and the individual;
Is authorised by law; or
The individual has given their explicit consent.

The Company will not carry out any automated decision-making or profiling using the personal data of a child.

13. PERSONAL DATA BREACHES WHERE THE COMPANY IS THE DATA CONTROLLER:

Where the Company establishes that a personal data breach has taken place, the Company will take steps to contain and recover the breach. Where a personal data breach is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

Where the personal data breach happens outside the UK, the Company shall alert the relevant supervisory authority for data breaches in the effected jurisdiction.

14. PERSONAL DATA BREACHES WHERE THE COMPANY IS THE DATA PROCESSOR:

The Company will alert the relevant data controller as to the personal data breach as soon as they are aware of it.

15. REPORTING PERSONAL DATA BREACHES

All data breaches should be referred to the **Mr. Gabriele Faggioli** uk.privacy@gigroup.com

16. COMMUNICATING PERSONAL DATA BREACHES TO INDIVIDUALS

Where the Company has identified a personal data breach resulting in a high risk to the rights and freedoms of any individual, the Company shall inform all affected individuals without undue delay.

The Company will not be required to tell individuals about the personal data breach where:

The Company has implemented appropriate technical and organisational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorised to access it, such as encryption.

The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.

It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

If you have a complaint or suggestion about the Company's handling of personal data then please contact the **Mr. Gabriele Faggioli** uk.privacy@gigroup.com

Alternatively you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

17. THE LAWFULNESS OF PROCESSING CONDITIONS FOR PERSONAL DATA

a) Consent of the individual for one or more specific purposes.
b) Processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
c) Processing is necessary for compliance with a legal obligation that the controller is subject to.
d) Processing is necessary to protect the vital interests of the individual or another person.
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
f) Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of personal data, in particular where the individual is a child.

All the Company's staff are responsible for satisfying themselves that there is a proper legal basis for them to process any Personal Data.

c) THE LAWFULNESS OF PROCESSING CONDITIONS FOR SENSITIVE PERSONAL DATA

a. Explicit consent of the individual for one or more specified purposes, unless reliance on consent is prohibited by EU or Member State law.
b. Processing is necessary for carrying out data controller's obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.
c. Processing is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving consent.
d. In the course of its legitimate activities, processing is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body, with a political, philosophical, religious or trade union aim and on condition that the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the consent of the individual.
e. Processing relates to personal data which are manifestly made public by the individual.
f. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
g. Processing is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.

h. Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.
i. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.
j. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.