

PRIVACY NOTICE – NEXT OF KIN CONTACT

THE COMPANY AND THE COMPANY POLICY

This policy is applicable to all businesses, offices and operations within the gap personnel group www.gap-personnel-group.com (referred to as The Company), including:

- Open Up Group Inc. – Company Reg – 8044442
- gap personnel Holdings Limited (including Hawk 3 Talent) – Company Reg – 3589208 – ICO - Z2057848 - <https://www.gap-personnel.com/>
- global personnel Limited – Company Reg – 11828264 – ICO - ZA841201 - <https://global-personnel.com/>
- gap technical Limited – Company Reg – 5646432 – ICO – ZA230558 - <https://www.gap-technical.com/>
- gap personnel (TELFORD) LTD – company Reg – 13377649 – ICO – ZB346100 - <https://www.gap-personnel.com/>
- Quattro Recruitment Limited t/a gap personnel – Company Reg – 7131120 – ICO – ZA015243 - <https://www.gap-personnel.com/>
- Quattro Healthcare Ltd t/a gap healthcare – Company Reg - 9389534 – ICO – ZA127351 - <https://www.gap-healthcare.com/>
- Driving Force Recruitment Limited - company Reg – 06538808 – ICO - Z1709668 - <https://www.driving-force.co.uk/>

Our parent company is Open Up Group Inc. which is a global human resources and staffing provider; Open Up Group Inc. 3F NBF Comodio Shiodome, 2-14-1 HigashiShimbashi, Minato-ku, Tokyo 105-0021.

The Company is a recruitment business which provides work-finding, recruitment, training and related services to its clients and work-seekers. The Company must process personal data so that it can provide these services – in doing so, the Company acts as a data controller. We will only use your personal data in accordance with the terms outlined in our contracts and our privacy notice.

1. COLLECTION AND USE OF PERSONAL DATA

The Company will collect your personal data and process your personal data for the purposes of emergency contact in the immediate health and safety interest of our applicant; or worker; or employee, including concerns of their wellbeing when the Company has been unable to contact the applicant; or worker; or employee for an extended period of time.

In some cases we may be required to use your data for the purpose of investigating, reporting and detecting crime and also to comply with laws. We may also use your information during the course of audits to demonstrate our compliance with certain industry standards.

In any case the Company must have a legal basis for processing your personal data. We will only use your personal data in accordance with the terms of our privacy notice.

1.1 COLLECTION OF DATA

Your personal details have been provided to us by another person (our applicant; or worker; or employee) who has indicated you as an emergency contact.

1.2 PURPOSE OF PROCESSING AND LEGAL BASES

The legal bases we rely upon when processing your personal data are:

Legal base	Example of purpose
Legal obligation	Does not apply
Contractual obligation	Does not apply
Legitimate interest	To be able to inform applicant; or worker; or employee's relative of emergency situation and/or to clarify concerns about their wellbeing
Consent	Does not apply
Public interest	Does not apply
Vital interest of data subject	To inform applicant; or worker; or employee's relative of emergency situation and/or to clarify concerns about their wellbeing

1.3 RECIPIENTS/S OF DATA

Where we need to share your personal and/or sensitive data, we have contracts and data sharing agreements in place with the recipients that require them to treat your information as confidential and ensure the continued protection of your data whilst in their possession. The Company will process your personal data and/or sensitive data, with the following recipients:

- a) Our parent company and any of our group companies;
- b) Governing bodies, law enforcement, regulators and any other authorities as required by law;
- c) Any organisations including trade bodies, associations, business partners of which we are registered members or licence holders, such as REC, GLAA, ALP, Sedex and Stronger Together;
- d) Our clients, either during the course of audits, or where illness, accident etc has occurred on our client's premises and it is in the wellbeing of applicant; or worker; or employee for our client, first aider or medical team onsite at the client's premises to discuss any medical situations directly with the next of kin;
- e) Master/Neutral vendor and/or other recruitment agencies and/or Employment Business within the supply chain, when applicable;
- f) Our software providers, including IT, CRM, Website, Marketing technology platforms and suppliers;
- g) Third party suppliers, e.g. business associates and professional advisers, such as external consultants, technical and IT support functions, payroll companies, pension provider, insurers, legal advisors, independent auditors and intermediaries;
- h) We may transfer your personal information to a third party as part of a TUPE transfer under The Transfer of Undertakings (Protection of Employment) Regulations 2006;
- i) We may transfer your personal information to a third party as part of a sale of some or all of our business and assets to any third party or a part of any business restructuring or reorganisation. However, we will take steps with the aim of ensuring that your privacy rights continue to be protected.

2. OVERSEAS TRANSFERS

The Company may transfer the information you provide to us to countries outside the European Economic Area ('EEA'). The EEA comprises the EU member states plus Norway, Iceland and Liechtenstein. The most common reason for this is since our parent company Open Up Group Inc. is based in Japan. Whenever your data is shared with Open Up Group Inc. it is done so through our UK based secure SharePoint system.

Whenever your data is shared, inside or outside of the EEA, we will take every step possible to ensure adequate protections are in place to ensure the security of your information.

3. AUTOMATED DECISION-MAKING DRAFT AMENDS

The company does not use automated decision-making, including profiling that would impact you in the capacity and purposes for which we hold your data. Should the company intend to change this process you will be notified in advance.

4. DATA ACCESS RESTRICTION AND RETENTION

The Company will retain your personal data and/or sensitive data only for as long as is necessary. Different laws require us to keep different data for different periods of time.

4.1 WHERE SERVICES HAVE NOT BEEN PROVIDED

If we have not provided the individual for which you are an appointed Next of Kin contact with our services, or had valuable contact with for two consecutive years, your personal data will be deleted from our systems save where we believe in good faith that the law or other regulation requires us to preserve it.

4.2 WHERE SERVICES HAVE BEEN PROVIDED

Your personal details may be included in several documents created during the course of our contract with the individual for which you are an appointed Next of Kin contact. To comply with legal requirements e.g. HMRC, UK Visas and Immigration, The Conduct of Employment Agencies and Employment Businesses Regulations 2003, Agency Workers Regulation, HSE and tax legislation, your data will be kept by The Company for 7 tax years from the last date on which services were provided to the individual for which you are an appointed Next of Kin contact.

Where the Company has obtained your consent to process your personal data and sensitive personal data we will do so in line with the relevant schedule detailed above. After expiry of that period your data will no longer be kept by The Company.

5. SECURITY PRECAUTIONS IN PLACE TO PROTECT THE LOSS, MISUSE OR ALTERATION OF DATA

We are committed to taking all reasonable and appropriate steps to protect the personal information that we hold from misuse, loss, or unauthorised access. We do this by having in place a range of appropriate technical and organisational measures, e.g.:

- a) encryption of our services and data;
- b) review our information collection, storage and processing practices, including physical security measures;
- c) restrict access to personal access to personal information;
- d) internal policies setting out our data security approach and training for employees, these include measures to deal with any suspected data breach.

Our systems are placed on servers dedicated to The Company, running on an industry standard virtualisation platform based on VMware. Our server provider, where we store most of the data, is ISO 27001 accredited and follows industry best practice and regularly patches and upgrades platforms. All servers that we use to store your data are placed in UK area and comply with the General Data Protection Regulation. Our security systems are kept up to date and align with the guidance to security information.

The server that holds the Candidate Portal is installed with an SSL certificate to protect your data. Once you are on the Candidate Registration Portal, a padlock icon will appear near the address bar of the browser you are using; this will confirm you are on our secure Candidate Portal system.

6. YOUR RIGHTS

Please be aware that you have the following data protection rights:

- a) The right to be informed about the personal data the Company processes on you;
- b) The right of access to the personal data the Company processes on you;
- c) The right to rectification of your personal data;
- d) The right to erasure of your personal data in certain circumstances;
- e) The right to restrict processing of your personal data;
- f) The right to data portability in certain circumstances;
- g) The right to object to the processing of your personal data that was based on a public or legitimate interest;
- h) The right not to be subjected to automated decision making and profiling; and
- i) The right to withdraw consent at any time.

Where you have consented to the Company processing your personal data and sensitive personal data you have the right to withdraw that consent at any time by completing on-line request ([click here](#)) or emailing Data Protection Officer dpo@gap-personnel.com

7. COMPLAINTS OR QUERIES

If you wish to complain about this privacy notice or any of the procedures set out in it please contact: Data Protection Officer by emailing dpo@gap-personnel.com

You also have the right to raise concerns with the Information Commissioner's Office (ICO) on 0303 123 1113 or at <https://ico.org.uk/concerns/> or any other relevant supervisory authority should your personal data be processed outside of the UK, if you believe that your data protection rights have not been adhered to.

PRIVACY NOTICE – NEXT OF KIN – VERSION 7 – 01.09.2022