

The Privacy Notice reflects the requirements of the General Data Protection Regulation (GDPR), which came into effect in the UK on 25 May 2018.

**Data Controller: DIG International Group**

**Data Protection Officer: Russell Evans**

DIG International Group collects and processes personal data relating to all its employees to manage the employment relationship. The Company is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

## What information does the Company collect?

The Company collects and processes a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- the terms and conditions of your employment;
- details of your qualifications, skills, experience, interview notes, references and employment history, including start and end dates, with previous employers and with the Company;
- information about your remuneration, including entitlement to benefits such as pensions, insurance and private healthcare cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK and overseas such as passport and visas;
- your eligibility to drive vehicles in the UK and insurance cover;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- details of your training records, including courses attended, certificates, certifications, application forms, enrolments and grant claims;
- information about medical, health conditions or vaccinations, including whether or not you have a disability for which the Company needs to make reasonable adjustments;
- details of your health and safety records, including drug and alcohol testing, tool box talks, incident reports and induction records;
- details of trade union membership; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

The Company collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the Company collects personal data about you from third parties, such as references supplied by former employers and information from criminal records checks permitted by law.

Data is stored in a range of different places, including in your personnel file, in the Company's HR management systems and in other IT systems including DIS's email system.

### Why does DIG process personal data?

The Company needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the Company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, the Company has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the Company to;

- run recruitment and promotion processes;
- 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;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- 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;
- 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;
- 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 Company 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;
- ensure effective general HR and business administration;
- provide references on request for current or former employees; □ respond to and defend against legal claims; and □ maintain and promote equality in the workplace.

Where the Company relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). Information about trade union membership is processed to allow the Company to operate checkoff for union subscriptions.

Where the Company processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the Company uses for these purposes is anonymised or is collected with the express consent of employees,

which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

## **Who has access to data?**

Your information will be shared internally, including the Human Resources Department, your line manager, managers in the business area in which you work and IT staff if access to the data is necessary for performance of their roles.

As an employer, we are legally obliged to share certain data about you with government agencies such as HMRC, ONS, DWP and Child Maintenance Service. The Company also shares your data with third parties in order to comply with client requirements, obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service. The Company may also share your data with third parties in the context of a sale or some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The Company also shares your data with third parties that process data on its behalf, in connection with the provision of benefits, insurance, private healthcare, professional award bodies, IT services and telecommunication providers.

Your data may be transferred to countries outside the European Economic Area (EEA) if you are assigned to work overseas and will be safeguarded by appropriate encryption measures.

## **How does the Company protect data?**

The Company takes the security of your data seriously. The Company has internal policies and access controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the Company engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

## **For how long does the Company keep data?**

The Company will hold your personal data for the duration of your employment]. The periods for which your data is held after the end of employment are set out in the DIG Data Protection policy.

## **Your rights**

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the Company to change incorrect or incomplete data;
- require the Company to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the Company is relying on its legitimate interests as the legal ground for processing; and
- ask the Company to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the Company's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact Russell Evans [russellevans@dig-ig.com](mailto:russellevans@dig-ig.com) or DIG International Group, Players Industrial Estate, Clydach, Swansea, SA6 5BQ.

If you believe that the Company has not complied with your data protection rights, you can complain to the Information Commissioner.

### **What if you do not provide personal data?**

You have some obligations under your employment contract to provide the Company with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the Company with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the Company to enter a contract of employment with you. If you do not provide other information, this will hinder the Company's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

### **Automated decision making**

Employment decisions are not based solely on automated decision making.