

General Data Protection Regulation (GDPR) Privacy Policy

D2 Global (known as the company) is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, under the General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act 2018. This policy sets out how the company deals with personal data, including personnel files and data subject access requests, and employees' obligations in relation to personal data.

Data Protection Officer

The CEO is the company's data protection officer and is responsible for the overall implementation of this policy. If employees have any questions about data protection in general, this policy or their obligations under it, they should direct them to the data protection officer.

Data Protection Principles

GDPR sets out key data principles that are to be followed in the handling of personal data. These principles are as follows:

- Lawfulness, fairness and transparency – all data must be fairly and lawfully processed in a transparent manner.
- Purpose limitation – all data must be processed for limited purposes and not in any manner incompatible with those purposes.
- Data minimisation – data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy- all data must be accurate and where necessary, 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.
- Storage limitation – data must not be kept longer than is necessary for the purposes for which the personal data are processed.
- Integrity and confidentiality (security)- data must be processed in a manner that ensures appropriate security of the personal data.
- Accountability - requires you to take responsibility for what you do with personal data and how you comply with the other principles.

Personal data

The Data Protection Act 1998 and GDPR applies to information that constitutes "personal data". Information is "personal data" if:

- A person can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

Consequently, automated and computerised personal information about employees held by employers is covered by the Act. Personal information stored physically (for example, on paper) and held in any "relevant filing system" is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered.

A "relevant filing system" means a well-structured manual system that amounts to more than a bundle of documents about each employee filed in date order, i.e., a system to guide a searcher to where specific information about a named employee can be located easily.

The Data Protection Act 1998 and GDPR applies to personal information that is "processed". This includes obtaining personal information, retaining, and using it, allowing it to be accessed, disclosing it and, finally, disposing of it in a confidential way.

The personal data that we collect.

- We may process data enabling us to get in touch with you ("contact data") The contact data may include phone number, title, and email address, in addition to your company's name and contact information. We may also collect feedback, comments and questions received from you in service-related communication and activities, such as meetings, phone calls, documents, and emails.
- From our websites we may collect IP-address and actions taken on the site.
- If you apply for a job at D2 Global, we collect the data you provide during the application process.
- We use cookies and web beacons ('Website Navigational Information') to collect information as you navigate the company's websites. Website Navigational Information includes standard information from your web browser, such as browser type and browser language; your Internet Protocol ("IP") address; and the actions you take on the company's websites, such as the web pages viewed, and the links clicked.

This information is used to make websites work more efficiently, as well as to provide business and marketing information to the owners of the site, and to gather such personal data as browser type and operating system, referring page, path through site, domain of ISP, etc. for the purposes of understanding how visitors use a website. Cookies and similar technologies help us tailor our website to your personal needs, as well as to detect and prevent security threats and abuse. If used alone, cookies and web beacons do not personally identify you.

The company may collect relevant sensitive personal information from employees for equal opportunities monitoring purposes. Where such information is collected, the company will anonymise it unless the purpose to which the information is put requires the full use of the individual's personal information. If the information is to be used, the company will inform employees on any monitoring questionnaire of the use to which the data will be put, the individuals or posts within the organisation who will have access to that information and the security measures that the company will put in place to ensure that there is no unauthorised access to it.

Our legal basis for collecting personal data.

Collecting personal data based on consents.

Any collection of personal data based on consent from the data subject will not be undertaken until written consent is obtained. All documentation related to the consent given by the individual will be stored and documented in our systems.

Collecting personal data based on contracts.

We use personal information for fulfilling our obligations related to contracts and agreements with customers, partners and suppliers.

Collecting personal data based on legitimate interest.

We may use personal data if it is considered to be of legitimate interest, and if the privacy interests of the data subjects do not override this interest. Normally, to establish the legal basis for data collection, an assessment has been made during which a mutual interest between D2 Global and the individual person has been identified. This legal basis is primarily related to our sales and marketing purposes. We will always inform individuals about their privacy rights and the purpose for collecting personal data.

Why do we collect and use personal data?

We collect and use personal data mainly for HR reasons about partners and persons seeking a job or working in our company. We may also use personal data for marketing purposes through our website.

We may use your information for the following purposes:

- Send you marketing communications which you have requested. These may include information about our products and services, events, activities, and promotions of our associated partners' products and services. This communication is subscription based and requires your consent.
- Send you information about the products and services that you have purchased from us.
- Reply to a 'Contact Us' or other web forms you have completed on the D2 Global website (e.g., to download a document/PDF).
- Follow up on incoming requests (customer support, emails, chats, or phone calls).
- Provide you with access and services related to D2 Global.
- Perform contractual obligations such as order confirmation, license details, invoice, reminders, and similar. The contract may be with D2 Global directly or with a D2 Global partner.
- Notify you about any disruptions to our services.
- Contact you to conduct surveys about your opinion on D2 Global products and services.
- Process a job application.

Personnel Files

An employee's personnel file is likely to contain information about their work history with the organisation and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the employee including address details and national insurance number.

There may also be other information about the employee located within the organisation, for example in their line manager's inbox or desktop; with payroll; or within documents stored in a relevant filing system.

The company will ensure that personal information about an employee, including information in personnel files, is securely retained. The company will keep hard copies of information in a locked filing cabinet or cupboard. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.

Special Category data

The GDPR defines special category data as

- personal data revealing racial or ethnic origin.
- personal data revealing political opinions.
- personal data revealing religious or philosophical beliefs.
- personal data revealing trade union membership.
- genetic data.
- biometric data (where used for identification purposes).
- data concerning health.
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

The company will not retain special category data without the express consent of the employee in question and will process special category data in accordance with GDPR special category data principles.

GDPR provides the following rights for individuals:

- **the right to access** - you can ask for copies of your personal data.
- **the right to rectification** - you can ask us to rectify inaccurate personal data and to complete incomplete personal data.
- **the right to erasure** - you can ask us to erase your personal data.
- **the right to restrict processing** - you can ask us to restrict the processing of your personal data.
- **the right to object to processing** - you can object to the processing of your personal data.
- **the right to data portability** - you can ask that we transfer your personal data to another organisation or to you.
- **the right to complain to a supervisory authority** - you can complain about our processing of your personal data.
- **the right to withdraw consent** - to the extent that the legal basis of our processing of your personal data is consent, you can withdraw that consent.

Data Subject Access Requests

An employee has the right to access information kept about them by the company, including personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee. Should an employee require access a subject access request must be made to the Data Protection Officer. Subject access requests can be emailed to info@d2-global.co.uk all subject access requests will be stored on the restricted access drive.

The company will inform each employee of:

- the types of information that it keeps about them.
- the purpose for which it is used; and
- the types of organisations that it may be passed to, unless this is self-evident (for example, it may be self-evident that an employee's national insurance number is given to HM Revenue & Customs).

The data protection officer is responsible for dealing with data subject access requests. The company will respond to any data subject access requests within 30 calendar days, this is calculated from the day the request is received until the corresponding calendar date in the next month. If the corresponding date falls on a weekend or a public holiday, the next working day will be regarded as the 30-day period.

The company may reserve its right to withhold the employee's right to access data where any statutory exemptions apply.

Examples of exemptions: where a reference given (or to be given) in confidence for employment, training or educational purposes. The exemption covers the personal data within the reference whether processed by the reference giver or the recipient.

Correction, updating and deletion of data.

The company has a system in place that enables employees to check their personal information on a regular basis so that they can correct, delete or update any date. If an employee becomes aware that the company holds any inaccurate, irrelevant or out-of-date information about them, they must notify the data protection officer immediately and provide any necessary corrections and/or updates to the information.

Any requests will be actioned within 30 days of receipt. The company may reserve its right to withhold the employee's right to rectify data where any statutory exemptions apply.

Data that is likely to cause substantial damage or distress.

If an employee believes that the processing of personal information about them is causing, or is likely to cause, substantial and unwarranted damage or distress to them or another person, they may notify the company in writing to the data protection officer to request the organisation to put a stop to the processing of that information.

Within 30 days of receiving the employee's notice, the company will reply to the employee stating either:

- that it has complied with or intends to comply with the request; or
- the reasons why it regards the employee's notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

If the request is upheld and processing is restricted, the company may still store the personal data, but not use it.

Monitoring.

The company may monitor employees by various means including, but not limited to, recording employees' activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. If this is the case, the company will inform the employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee will usually be entitled to be given any data that has been collected about them. The company will not retain such data for any longer than is necessary.

In exceptional circumstances, the company may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the company by the activity being monitored and where the information cannot be obtained effectively by any non-intrusive means (for example, where an employee is suspected of stealing property belonging to the company). Covert monitoring will take place only with the approval of the data protection officer or a director.

Data Processors obligations regarding personal information.

If a data processor acquires any personal information in the course of their, they must ensure that:

- the information is accurate and up to date, insofar as it is practicable to do so.
- the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- the information is secure.

In particular, an employee should ensure that they:

- uses password-protected and encryption in transit software for the transmission and receipt of emails.
- locks files in a secure cabinet.

Where information is disposed of, data processors should ensure that it is adequately destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder.

Hard copies of information will be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an employee acquires any personal information in error by whatever means, they shall inform the Data Protection Officer immediately and, if it is not necessary for them to retain that information, arrange for it to be handled by the appropriate individual within the organisation.

The GDPR primarily applies to the European Economic Area (the EEA) with some exceptions. The GDPR restricts transfers of personal data outside the EEA, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies. Where an employee is required to disclose personal data to any other country, they must ensure first that there are adequate safeguards for the protection of data in the host country, these safeguards must also be prior approved by the Data Protection Officer.

An employee must not take any personal information away from the company's premises save in circumstances where they have obtained the prior consent of the data protection officer to do so. If an employee is in any doubt about what they may or may not do with personal information, they should seek advice from the data protection officer. If they cannot get in touch with the data protection officer, they should not disclose the information concerned.

Training

The company provides compulsory training on data protection issues to all employees who handle personal information in the course of their duties at work. The company will continue to provide such employees with refresher training on a regular basis. Such employees are also required to have confidentiality clauses in their contracts of employment and will be asked to confirm they have read, understood and will comply with D2 Global General Data Protection Regulation (GDPR) Privacy Policy and the Data Protection & GDPR procedure.

Consequences of non-compliance

The Information Commissioner has the power to issue a monetary penalty for an infringement of the provisions of Part 3 of the Act – Law Enforcement Processing. Any penalty that we issue is intended to be effective, proportionate and dissuasive, and will be decided on a case by case basis.

Under Part 6 of the Act, there are two tiers of penalty for an infringement of Part 3 - the higher maximum and the standard maximum.

The higher maximum amount is £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

The higher maximum amount can apply to any failure to comply with any of the data protection principles, any rights an individual may have under Part 3 or in relation to any transfers of data to third countries.

If there is an infringement of other provisions, such as administrative requirements of the legislation, the standard maximum amount will apply, which is £8.7 million or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

All employees are under an obligation to ensure that they have regard to the data protection principles (see above) when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, the organisation will treat this as gross misconduct and instigate its disciplinary procedures.

Taking employment records off site

An employee must not take employment records off site (whether in electronic or paper format) without prior authorisation from the data protection officer.

An employee may take only certain employment records off site. These are documents relating to disciplinary or grievance meetings that cannot be held on site/meetings with occupational health/discussions surrounding the sale of the business or specific monitoring purposes/seeking professional advice. An employee may also take employment records off site for any other valid reason given by the data protection officer.

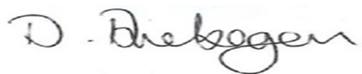
Any employee taking records off site must ensure that they do not leave their laptop, other device or any hard copies of employment records on the train, in the car or any other public place. They must also take care when observing the information in hard copy or on-screen that such information is not viewed by anyone who is not legitimately privy to that information.

Where laptops are taken off site, employees must follow the company's relevant policies relating to the security of information and the use of mobile devices.

Review of Policy & Procedures

This policy along with corresponding procedures will be reviewed at regularly intervals for its effectiveness and compliance will be monitored through regular audits of the company's activities.

Signed:



CEO

Date: 11th January 2023
(Rev: 4)