General Data Protection Regulation (GDPR) Privacy Policy

D2-UK-BMS-POL-001

14/11/2024

Document Control Sheet and Version History

Version	Date	Owner	Comments
1.0	14/11/2024	Patricia Rogers	First Issue. Combined RISQS document D2/033DATA and D2-UK-BMS-POL-016 as they had similar information on GDPR

Version	Prepared by	Approved by
1.0	Name: Patricia Rogers Role: HR Manager **Date**: 14/11/2024	Name: Simon Blair Role: COO **Date**: 15/11/2024

Contents

1. Purpose

The purpose of this document is to establishes an effective, accountable and transparent procedure for ensuring compliance with the requirements of the under the General Data Protection Regulation (GDPR).

2. Scope

This procedure applies to all employees of the company and contractors both full-time and part-time and all third parties responsible for the processing of persona data on behalf of D2 Global Limited.

3. Definitions and Terminology

Definitions for any specific terms or jargon used in the policy to ensure all readers have a clear understanding.

Term of reference	Definition/Description/Explanation of Term
GDPR	General Data Protection Regulation
DPIA	Data Protection Impact Assessment

4. Policy Statement

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.

GDPR sets out key data principles that are 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 or 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.

5. Responsibilities

Directors/Senior Leadership Team:

- Ensuring the alignment of the policy and provide the necessary resources.
- Assigning relevant roles and responsibilities.
- Ensuring that managers and supervisors undertake training relevant to their responsibilities.

Data Protection Office:

- Ensure that the organization complies with data protection laws, regulations, and internal policies.
- Conduct regular audits and assessments to verify data processing activities are lawful and follow best practices.
- Advise the organization on its obligations under relevant data protection laws.
- Ensuring that employees undertake training relevant to their responsibilities
- Advising on Data Protection Impact Assessments
- Liaising with Regulatory Authorities
- Coordinate the investigation and response to data breaches,

Data Processors:

- Implementing the policy in all company procedures.
- Understanding the importance of the GDPR and how it sits within their role.
- Undertaking training relevant to their responsibilities
- Issuing of relevant mandatory training to new employees

Capability Leads/Line Managers:

- Undertaking training relevant to their responsibilities.
- Implementing this policy throughout their capability
- Understanding the importance of the GDPR and how it sits within their role.

Employees/Subcontractors:

- Adhering to this policy
- Understanding the importance of the GDPR and how it sits within their role.

6. Procedure

6.1 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:

- Sending marketing communications which have been 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 information about the products and services 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 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 about any disruptions to our services.
- to conduct surveys about opinion on D2 Global products and services.
- Process a job application.

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.

D2 Global 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.

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 contact data. The contact data may include phone number, title, and email address, in addition to any company name and contact information. We may also collect feedback, comments and questions received regarding 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.

- For applicants applying for a job at D2 Global, we collect the data provide during the application process.

- We use cookies and web beacons ('Website Navigational Information') to collect information as from 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 taken 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.

7. Our legal basis for collecting personal data.

7.1 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.

7.2 Collecting personal data based on contracts.

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

7.3 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. To establish the legal basis for data collection, a Legitimate Interests Assessment D2-UK-BMS-FRM-020 is completed prior to the data being collected in which a mutual interest between D2 Global and the individual person has to be identified. All Legitimate Interests Assessment must be completed in full and signed off by the Data Protection Officer.

Once authorised the Legitimate Interests Assessment form will be filed in the GDPR file on the restricted drive and linked to the relevant record on the GDRP Data Control Log.

8. 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

9. 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.

10. 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.

11. Data subject consent

D2 Global Ltd will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned.

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 HR@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.

Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, D2 Global Ltd is committed to seeking such consent. All consents will be filed on the in the restricted access GDPR folder and linked to the GDPR Data Control Log.

12. 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.

13. 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 to store the personal data, but not use it.

14. External Privacy Notices

D2 Global external website will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law

15. Third Party Organisations

There must be a written contract with any third-party data processing D2 Global data under GPDR. The contract must set out the following:

- The subject matter of the processing
- The duration of processing
- The nature of processing
- The purpose of processing
- The type of personal data to be processed
- The categories of data subjects whose data is to be processed
- The rights and obligations of the data controller

The contract must include the following instructions to the data processor:

- The processor must only process the data on the instructions of the controller
- Any individual processing data for the processor must have a commitment to confidentiality

- The processor must take appropriate security measures
- The processor must assist the controller to comply with data subjects' rights, including reporting any personal data breaches to the controller immediately
- The controller identifies whether the personal data should be deleted or returned to the controller at the end of the provision of services
- The processor must assist the controller with the provision of information for audit or inspection purposes

All copies of third party agreements must be saved in the GDPR restricted access folder and linked to the GDPR Data Control Log.

16. Data Protection by Design

When designing new systems or processes and/or when reviewing or expanding existing systems or processes, each process must go through an approval stage before continuing and a D2-UK-QMS-FRM-222 GDPR Data Protection Impact Assessment (DPIA) must completed. The subsequent findings of the DPIA must then be submitted to the Directors for review and approval.

Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection Officer to assess the impact of any new technology uses on the security of personal data.

17. 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.

18. Marketing

D2 Global Ltd will not send direct marketing material to individuals without first obtaining consent. The data subject must be informed at the point of first contact that they have the right to opt out, at any stage. If the data subject puts forward an objection, digital marketing related processing of their personal data must

cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted. Where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of consent to carry out digital marketing but they are given the opportunity to opt-out.

19. Childrens data

Children under the age of 14 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

20. Data Retention

To ensure fair processing, personal data will not be retained by D2 Global Ltd for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which we need need to retain personal data is set out in the GDRP Data Control Log. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

21. Data subject Requests

If an individual makes a request relating to any of the rights listed below D2 Global will respond within 30 days of the request.

Information access.

Objection to processing.

Objection to automated decision-making and profiling.

Restriction of processing.

Data portability.

Data rectification.

Data erasure.

Each such request will be considered in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data subject requests may be made in writing/email marked for the attention of the Data Protection Officer (HR@d2-global.com)

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

21.1 Extended the time for data subject requests

The time to respond to a subject request may be extended by a further two months if the request is complex or if a number of requests has been received from an individual. If an extension is required the individual will be informed within one month of receiving the request and an explanation of why the extension is necessary will be provided.

22. Third party requests

The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them.

In these cases, the third party will be asked to provide evidence of the entitlement. This might be a written authority to make the request or it might be a more general power of attorney.

If there is no evidence that a third party is authorised to act on behalf of an individual, if possible the individual should be contacted direct and asked to provide adequate evidence the third party is acting on their behalf , the individual must also provide confirmation that they have requested the data subject request.

23. Data Quality

D2 Global will adopt all necessary measures to ensure that the personal data it collects, and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject.

The measures adopted to ensure data quality include:

Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.

Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.

The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.

24. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for purposes such as the prevention and detection of crime or by the order of a court or by any rule of law:

If D2 Global receives a request from a court or any regulatory or law enforcement authority for information relating to a D2 Global employee contact, the Data Protection Officer must be notified immediately and advise on how to process the request will be given.

25. 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.

26. Data Protection Training

All D2 Global employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, regular data protection training and procedural guidance will be provided for staff.

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.

27. Complaints handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period.

28. 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.

29. Review

This policy is reviewed at least every year to ensure it remains effective, relevant, and appropriate to our organisation, and reflect legislative requirements, or earlier if:

There is a newly identified risk to the business.

A significant incident or nonconformity occurs.

Audit results demonstrate that the procedure failed to deliver the required outcomes.

There are changes in associated legislation.

There is evidence that the procedure is not having a positive impact on related indicators.

30. Records

All documentation and records generated are retained and managed in accordance with the Business Document Management Policy D2-GLB-QMS-POL-00001

31. Appendices/Document Reference

D2-UK-QMS-FRM-222 GDPR Data Protection Impact Assessment

D2-UK-BMS-FRM-020 Legitimate Interests Assessment

GDPR Data Control Log

General Data Protection Regulation (GDPR)