DATA PROTECTION POLICY

Policy No: 28

Last Reviewed April 2022

1. INTRODUCTION

1.1 Protocol need to collect and use certain types of information about staff, clients and other individuals who come into contact with the company in order to operate. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

1.2 This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this within the Data Protection Act 2018.

1.3 We regard the lawful and correct treatment of personal information as very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. We ensure that our organisation treats personal information lawfully and correctly.

1.4 The General Data Protection Regulation (GDPR), as supplemented by the Data Protection Act DPA 2018 (DPA), is the main piece of legislation that governs how Protocol collects and processes personal data. Failure to comply with this legislation may have severe consequences for the Organisation, including potential fines of up to €20 million or 4% of the total worldwide annual turnover, whichever is higher.

1.5 Protocol will, through appropriate management, ensure strict application of criteria and controls:

- Observe fully the conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- Provide clear and concise details of how and why we process data within contracts, terms and conditions, system and privacy policies
- Ensure the quality of information used
- Apply strict checks to determine the length of time information is held
- Ensure that the rights of people about whom information is held, can be fully exercised under the act (these include: the right to be informed that processing is being undertaken, the right of access to one's personal information, the right to prevent processing in certain circumstances and the right to correct, rectify, block or erase information which is regarded as wrong information)
- Take appropriate technical and organisational security measures to safeguard personal information
- Provide individuals that request it, within a maximum of 30 days from request, with access to personal information held about them
- Correct or erase any information on an individual that is inaccurate or misleading
- Not use information for a purpose which is incompatible with the original purpose for which permission was given by the data subject
- Obtain clear, express permission for handling and using 'sensitive' personal data such as race, ethnicity, political opinions, religious beliefs, trade union membership, state of health both physical and mental, sexual life, criminal convictions and sentences and allegations of criminal behaviour

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information
- Allocate such resources as may be required to ensure the effective operation of the Policy.

1.6 In addition, Protocol ensures that:

- there is someone with specific responsibility for Data Protection within the Organisation
- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- everyone managing and handling personal information is appropriately trained to do so
- everyone managing and handling personal information is appropriately supervised
- anybody wanting to make enquiries about handling personal information knows what to do
- queries about handling personal information are promptly and courteously dealt with
- methods of handling personal information are clearly described
- a regular review and audit are made of the way personal information is held, managed and used
- methods of handling personal information are regularly assessed and evaluated
- performance with handling personal information is regularly assessed and evaluated
- a breach of the rules and procedures identified in this Policy may lead to disciplinary action being taken against the members of staff concerned.

2. CONTACT

2.1 The Data Protection Officer is responsible for overseeing the implementation and review of this Policy (and the related policies and procedures). They can be contacted as follows:

- data@protocol.co.uk.

3. DATA PROTECTION PRINCIPLES

3.1 Protocol is committed to processing data in accordance with its responsibilities under the Data Protection Act. Protocol must ensure that personal data shall be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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 it is processed, is erased or rectified without delay;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

- 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.

3.2 Additionally Protocol must ensure that:

- Personal data is not transferred outside of the EEA (which includes the use of any website or application that is hosted on servers located outside of EEA) to another country without appropriate safeguards being in place

- Data subjects to able exercise their rights in relation to their personal data.

3.3 Protocol, as the data controller, is responsible for, and must be able to demonstrate, compliance with the other data protection principles.

4. LAWFUL PROCESSING

4.1 In order to collect and process personal data for any specific purpose, Protocol must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may also have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, consulted, used or otherwise processed.

4.2 Processing personal data will only be lawful where at least one of the following lawful bases applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes

- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of a data subject prior to entering into a contract

- The processing is necessary to comply with a legal obligation to which the controller is subject

- The processing is necessary to protect the vital interests of the data subject or another person

- The 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 controller.

- The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests and fundamental rights and freedoms of the data subject which require protection of personal data, especially were the data subject is a child.

5. FAIR OBTAINING AND PROCESSING

5.1 Protocol will ensure that as far as practicable, all individuals whose details are processed are aware of the way in which that information will be obtained, held, used and disclosed. Whenever possible, individuals will be informed of the potential recipients of the information. Processing of personal information will be fair and lawful (detailed in our Privacy Policy), and in addition, it is our policy that individuals will not be misled regarding the purposes to which the information is processed.

6. INFORMATION QUALITY AND INTEGRITY

6.1 We will endeavour to process personal information, which is accurate, current and is of good quality. Information that is obtained by us will be adequate and not excessive for the purpose for which it is processed. In addition, information will be kept for no longer than is necessary for the purpose or purposes for which it was obtained.

6.2 It is the responsibility of all staff members to ensure all data being processed is correct and up to date.

7. SECURITY OF PERSONAL DATA

7.1 The personal data collected and processed must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing. Protocol will continue to develop, implement and maintain appropriate technical and organisational measures for the processing of personal data taking into account the:

- nature, scope, context and purposes for such processing
- volume of personal data processed
- likelihood and severity of the risks of such processing for the rights of data subjects

7.2 Employees are responsible for ensuring the security of the personal data processed by you in the performance of your duties and tasks. You must ensure that you follow all policies and procedures in place to maintain the security of personal data from collection to destruction.

7.3 You must ensure that the confidentiality, integrity and availability of personal data are maintained at all times:

- Confidentiality: means that only people who need to know and are authorised to process any personal data can access it
- Integrity: means that personal data must be accurate and suitable for the intended purposes
- Availability: means that those who need to access the personal data for authorised purposes are able to do so

7.4 You must ensure that you observe and comply with our Information Security Management System.

7.5 You must not attempt to circumvent any administrative, physical or technical measures implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence.

8. REPORTING DATA BREACHES

8.1 In certain circumstances, the DPA will require Protocol to notify the ICO, and potentially data subjects, of any personal data breach.

8.2 Protocol has put in place appropriate procedures to deal with any data breach and will notify the ICO and/or data subjects where it is legally required to do so.

8.3 If you know or suspect that a data breach has occurred, you must contact the Data Protection Officer, your line manager and the IT Helpdesk, immediately to report it and obtain advice, and take all appropriate steps to preserve evidence relating to the breach.

8.4 You must ensure that you observe and comply with the data breach procedure.

9. SHARING DATA

9.1 You are not permitted to share personal data with third parties unless Protocol has agreed to this in advance, this has been communicated to the data subject in a privacy policy or fair processing agreement beforehand and, where such third party is processing the personal data on our behalf, the Protocol has undertaken appropriate due diligence of such processor and entered into an agreement with the processor that complies with the DPA's requirements for such agreements.

9.2 The transfer of any personal data to an unauthorised third party would constitute a data breach. Do not share any personal data with third parties, including the use of freely available online and cloud services for work-related purposes, unless you are certain that the conditions outlined above apply. Seek advice from the Data Protection Officer if you are unsure.

10. TRANSFER OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

10.1 The DPA prohibits the transfer of personal data outside of the EEA in most circumstances in order to ensure that personal data are not transferred to a country that does not provide the same level of protection for the rights of data subjects. In this context, a "transfer" of personal data includes transmitting, sending, viewing or accessing personal data in or to a different country.

10.2 Protocol does not transfer data outside of the EEA. Should the requirement to do so change we may only do so if one of the following conditions applies:

- the European Commission has issued an "adequacy decision" confirming that the country to which we propose transferring the personal data ensures an adequate level of protection for the rights and freedoms of data subjects (this applies to only a small number of countries)
- appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses that have been approved by the European Commission, an approved code of conduct or certification mechanism
- the data subject has given their explicit consent to the proposed transfer, having been fully informed of any potential risks
- the transfer is necessary in order to perform a contract between Protocol and a data subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject in circumstances where the data subject is incapable of giving consent
- the transfer is necessary, in limited circumstances, for Protocol's legitimate interests

10.3 You must ensure that you do not transfer any personal data outside of the EEA except in the circumstances set out above and provided that Protocol has agreed to this in advance.

11. DATA SUBJECTS RIGHTS AND REQUESTS

11.1 The GDPR/DPA provides data subjects with a number of rights in relation to their personal data. These include:

- Right to withdraw consent: where the lawful basis relied upon by Protocol is the data subject's consent, the right to withdraw such consent at any time without having to explain why
- Right to be informed: the right to be provided with certain information about how we collect and process the data subject's personal data (through our Privacy Policy)
- Right of subject access: the right to receive a copy of the personal data that we hold, including certain information about how Protocol has processed the data subject's personal data
- Right to rectification: the right to have inaccurate personal data corrected or incomplete dated completed
- Right to erasure (right to be forgotten): the right to ask the Protocol to delete or destroy the data subject's personal data if: the personal data is no longer necessary in relation to the purposes for which they were collected; the data subject has withdrawn their consent (where relevant); the data subject has objected to the processing; the processing was unlawful; the personal data have to be deleted to comply with a legal obligation; the personal data was collected from a data subject under the age of 13, and they have reached the age of 13
- Right to restrict processing: the right to ask Protocol to restrict processing if: the data subject believes the personal data is inaccurate; the processing was unlawful and the data subject prefers restriction of processing over erasure; the personal data is no longer necessary in relation to the purposes for which it was collected but they are required to establish, exercise or defend a legal claim; the data subject has objected to the processing pending confirmation

of whether the Protocol's legitimate interests grounds for processing override those of the data subject

- Right to data portability: in limited circumstances, the right to receive or ask for their data to be transfered to a third party, a copy of the data subject's personal data in a structured, commonly-used machine-readable format

- Right to object: the right to object to processing where the lawful basis for processing communicated to the data subject the Protocol's legitimate interests and the data subject contests those interests

- Right to object to direct marketing: the right to request that we do not process the data subject's personal data for direct marketing purposes

- Right to object to decisions based solely on automated processing (including profiling): the right to object to decisions creating legal effects or significantly affecting the data subject which is solely by automated means, including profiling, and the right to request human intervention

- Right to be notified of a personal data breach: the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights or freedoms

- Right to complain: the right to make a complaint to the ICO or another appropriate supervisory authority

11.2 You must be able to identify when a request has been made and must verify the identity of the individual making a request before complying with it. You should be wary of third parties deceiving you into providing personal data relating to a data subject without their authorisation.

11.3 You must immediately forward any request made by a data subject (even if you are uncertain whether it represents a request as set out above) to the Data Protection Officer.

11.3.1 Protocol will respond positively to subject access requests, replying as quickly as possible, and in any event within the 30-day time limit. Requests are to be made in writing to data@protocol.co.uk.

11.3.2 We will only disclose personal data to the data subject, or to those recipients listed through consent of the data subject, or whenever it is otherwise permitted by law to do so. The organisation will always seek the permission of the data subject, where it is required by law to do so.

12. ACCOUNTABILITY AND RECORD KEEPING

12.1 Protocol is responsible for and must be able to demonstrate compliance with the data protection principles and other obligations under the GDPR. This is known as the 'accountability principle'. Protocol must ensure that it has adequate resources, systems and processes in place to demonstrate compliance with it's obligations including:

- appointing a suitably qualified and experienced Data Protection Officer (DPO) and providing them with adequate support and resource

- ensuring that at the time of deciding how Protocol will process personal data, and throughout its processing, implementing appropriate technical and organisational measures that are designed to ensure compliance with the data protection principles (known as 'Data Protection by Design')

- ensuring that, by default, only personal data that are necessary for each specific purpose are processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal data (known as 'Data Protection by Default')

- ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, an assessment of those risks has been carried out and is taking steps to mitigate those risks, by undertaking a 'Data Protection Impact Assessment' (see below)

- integrating data protection into internal documents, privacy policies and fair processing notices
- regularly training the employees on the GDPR, this policy and related policies and procedures, and maintaining a record of training completion by members of staff
- testing the measures implemented and conducting periodic reviews to assess the adequacy and effectiveness of this policy.

12.2 Protocol must keep full and accurate records of all its processing activities in accordance with the GDPR's requirements.

12.3 You must ensure that you have undertaken the necessary training provided and, where you are responsible for other members of staff, that they have done so.

12.4 You must further review all the systems and processes under your control to ensure that they are adequate and effective for the purposes of facilitating compliance with our obligations under this policy.

13. DIRECT MARKETING

13.1 Direct marketing is defined in section 122(5) of the Data Protection Act 2018 as:

"the communication (by whatever means) of advertising or marketing material which is directed to particular individuals".

This covers all advertising or promotional material. In practice, all relevant electronic messages (eg calls, faxes, texts and emails) who are directed to someone fall within this definition.

13.2 Routine customer service messages do not count as direct marketing – in other words, correspondence with customers to provide information they need about a current or past contract or registration (eg information about service interruptions, delivery arrangements, changes to terms and conditions). General branding, logos or straplines in these messages do not count as marketing.

13.3 Protocol must ensure that it has appropriate consent from individuals to send them direct marketing communications, and that when a data subject exercises their right to object to direct marketing it has honoured such requests promptly.

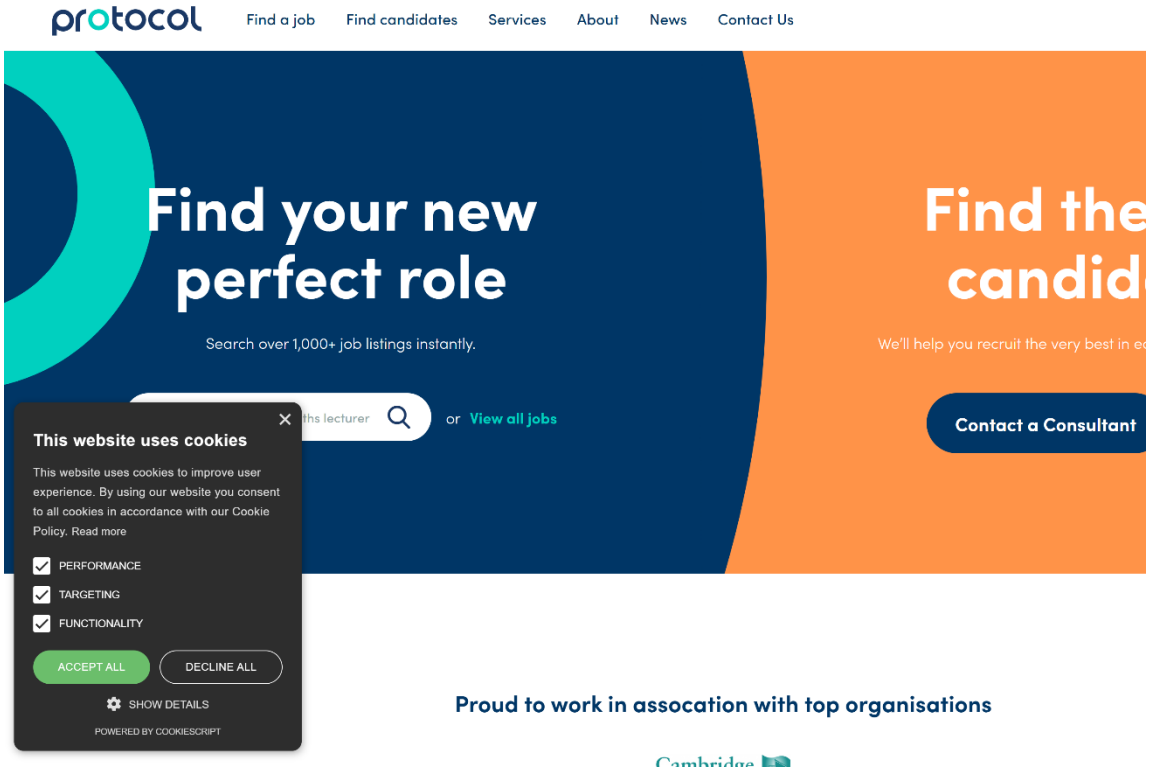
13.4 You must ensure that you understand or consult with the Data Protection Officer regarding legal obligations in relation to direct marketing a new service or brand before embarking upon any direct marketing campaign.

14. COOKIE POLICY

14.1 **What are cookies and how do we use them?** A "cookie" is a bite-sized piece of data that is stored on your computer's hard drive. Nearly all websites use them and rest assured, they do not harm your system. We use cookies to track visitor activity to help ensure everyone gets the best user journey experience when visiting our website and you can affectively access the information you visited us for. We can use the information from cookies to ensure we present visitors with options tailored to their preferences on their next visit. We can also use cookies to analyse traffic and for advertising purposes. If you want to check or change what types of cookies you accept, this can usually be altered within your browser settings or you visit our Cookie Consent System which you will see on the bottom left side side of our website.

14.2 **How to manage or reject cookies:** When you first visit our website, you will be presented with a pop up asking whether or not you consent for some cookies through our Cookie Consent System. You may also use your browser's privacy settings to do this. However please note that by rejecting all cookies through your browser's privacy settings, you may not be able to take full advantage of all our website's features. Each browser is different, so check the "Help" menu of your browser to learn how to change your cookie preferences.

You are able to update your given consent at any time by visiting our Cookie Consent System – see screenshot below:



Instead of using our Cookie Consent System, you may choose to opt-out of cookies which are not strictly necessary to perform basic features of our site by changing your browser settings. If you use our Cookie Consent System to update your choice of cookies, please note that this does not result in deletion of already placed cookies on your device. So, if you want to delete such cookies you may delete them in your browser's privacy settings.

If you choose to delete all cookies through your browser's privacy settings, this will also delete any placed opt-out cookie on your computer and you may need to actively opt-out again.

If you would like more information on cookies, including how to disable them, please refer to aboutcookies.org. You will also find details on how to delete cookies from your computer.

For a full list of Protocol cookies, please visit here

Report Ends