Reference	BWT - POL 00
Version	V.3
Issue Date	01/05/2018
Approved	MD

BLACK WATCH TACTICAL LTD

Data Protection Policy

GDPR (General Data Protection Regulation) – Processing of personal data

As you may be aware, new rules come into effect on the 25th of May 2018 regarding how we use and store your personal information. To comply with these regulations, there must be a lawful basis for us to, collect, process and store any personal data that you provide to us for the provision of Security Services.

Your rights

You have the right to object to how we process your personal information. You also have the right to access, correct, sometimes delete and restrict the personal information that we use. In addition, you have the right to complain to us and to the data protection regulator. You can get in touch with us by Telephone on 0800 001 6297 47 Dales Lane Whitefield Manchester M45 7JQ info@blackwatch-tactical.co.uk

1. PURPOSE

This policy applies to BWT in England. BLACK WATCH TACTICAL LTD is registered with the Information Commissioner and complete details of the BWT current entry on the Data Protection Register can be found on the notification section of the Information Commissioners web site. www.dataprotection.gov.uk. Our registration number is ZA161777 .

2. RESPONSIBILITY

The Director is responsible for ensuring that this policy is applied within the association. The Management Rep is responsible for maintenance, regular review and the updating of this policy.

3. STATUS OF THE POLICY

This document sets out the BWT policy and procedures to meet the requirements of the Data Protection Act 1998. It will be made available to employees.

Personal data covers both facts and opinions about the individual. With processing, the definition surrounding the intentions of the **data controller** towards the individual, are far wider than before. For example, it incorporates the concepts of 'obtaining', holding' and 'disclosing'. BWT Staff or others who process or use personal information must ensure that they follow these principles at all times.

4. THE DATA CONTROLLER

The Management Rep is ultimately responsible for Data Protection, but the BWT Director of Resources is regarded as the main Data Controller. In practice local Regional staff are designated as local data protection officers to deal with day to day matters and ensure they comply with the Data Protection Act on an ongoing basis. They will often look to Course Managers for support in this.

5. SUBJECT CONSENT

In many cases, BWT can only process personal data with the consent of the individual and if the data is sensitive, express consent must be obtained. Agreement to the BWT processing some specified categories of personal data is a condition of acceptance and a condition of employment for staff. For example, this includes information about previous criminal convictions, in accordance with the Rehabilitation of Offenders Act 1974.

(GDPR 01) approved by MD

6. STAFF RESPONSIBILITIES

This policy will not be incorporated into contracts of employment, but it is a condition of employment that employees will abide by the rules and policies made by BWT from time to time. Any failures to follow this policy can therefore result in disciplinary proceedings. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the Data Controller. If raising the issue with the Data Controller does not resolve it the matter should be raised as a formal grievance.

6.1. **Specific Staff Responsibilities**

All staff, including temp and staff such as security persons, have a responsibility for:

- Checking that any information that they provide to BWT in connection with their employment is accurate and up to date.
- Informing the BWT of any changes to information, which they have provided, i.e. changes of address, bank details, etc.
- Informing BWT Of any errors or changes in staff information.
- When staff hold or process information they should comply with the following Data Protection Guidelines:

All staff are responsible for ensuring that:

- Any personal data, which they hold, is kept securely, for example:
- kept in a locked filing cabinet;
- in a locked drawer;
- if it is computerised, be password protected;
- kept only on disk, which is itself kept securely.

- Personal information is not disclosed either orally or in writing
- Accidentally or otherwise to any unauthorised third party.
- Any unauthorised disclosure will be investigated as a disciplinary matter, and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member, as unauthorised disclosure can be a criminal offence.

6.2. **Staff Use of Personal Data Off-Site, On Home Computers or at Remote Sites**

Employees processing personal data off-site should ensure they take reasonable precautions to prevent the data from being accessed, disclosed or destroyed as a result of any act or omission on their part. They should notify the Data Controller immediately in the event of any loss or theft.

7. THIRD PARTIES

Any personal data which the Receives and processes in relation to third parties, such as visitors, employers, enquirers and other individuals on mailing lists etc. will be obtained lawfully and fairly and dealt with in accordance with the principles and conditions of the Act. Employees should obtain explicit consent from third party data subjects to process such personal data for the purposes expressed and should ensure that there is a mechanism for

data subjects to gain access to data about themselves, to prevent the processing of such data for the purposes of direct marketing and to object to the disclosure of such data.

8. Personal Data

Personal data should be transferred under conditions of security commensurate with the anticipated risks and appropriate to the type of data held. Personal data held electronically should be appropriately backed up and stored securely to avoid incurring liability to individuals who may suffer damage or distress as a result of the loss or destruction of their personal data.

Any disposal of personal data will be conducted in a secure way, normally by shredding. All computer equipment or media to be sold or scrapped must have had all personal data completely destroyed, by re-formatting, overwriting or degaussing (a method of erasing data held on magnetic media).

8.1. Retention of Data

The BWT will keep different types of information for differing lengths of time, depending on legal, academic and operational requirements.

8.2. Transfer of Data outside the UK

BWT Does not transfer personal data outside the UK without the express consent of the data subject.

If you have any further questions about the information that we are required to hold, or wish to request access or changes to your data, please contact us at the office.