BSAP REGIMENTAL ASSOCIATION UNITED KINGDOM BRANCH

DATA PROTECTION POLICY

Policy prepared by: Alan Toms

Approved by Executive Committee: 19th May 2018

Introduction

The BSAP Regimental Association United Kingdom Branch (BSAPRA UK) needs to gather and use certain information about individuals who are members of the BSAPRA UK and their partners in order to properly administer the Branch and regulate and organise its activities.

The Data Protection legislation describes how organisations must collect handle and store personal information.

This applies regardless of whether the data is stored electronically, on paper or on other materials.

Personal Data means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. (eg email address)

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier.

The Data must

1) Be processed lawfully and fairly
2) Be obtained only for specific lawful purposes.
3) Be relevant, adequate and not excessive
4) Be accurate and kept up to date
5) Not be held for longer than necessary
6) Be processed in accordance with the rights of data subjects
7) Be protected in appropriate ways.

Responsibilities

All members of the executive committee have some responsibility for ensuring data is collected, stored and handled appropriately.

Data Controller is a natural or legal person who alone or jointly with others determines the means and purpose of the processing of personal data, for the BSAPRA UK this is the Executive Committee of the Branch.

Data Processor is the person or persons which process data on behalf of the controller.

'Processing' in relation to personal data means an operation or set of operations which is performed on personal data, or on sets of personal data such as:
Collection, recording, organisation structure or storage
Adaption or alteration
Retrieval, consultation

For the BSAPRA UK those persons who are currently data processors are Alan Toms, James Harris, Steve Acornley, Bertie Cubitt, Michael Cozens.

IT Officer

Currently Deputy Chairman Alan Toms has responsibility for advising the committee of the security requirements for data protection

General Guidelines for Data Storage

The only persons able to access data stored by BSAPRA UK should be those who need it to carry out their duties as executive committee members.

Data should not be shared informally or disclosed to unauthorised persons outside the executive committee

Committee members should keep all data secure by taking sensible precautions and following these guidelines, in particular **strong passwords** must be used and never shared.

Data will be reviewed and updated regularly and deleted if no longer required.

Data stored on paper, including print outs of electronic data should be kept in a secure place and shredded or destroyed when no longer needed.

Data must be held in as few places as possible, unnecessary data sets should not be created.

UK Branch membership data should only be stored in a central secure location, the UK Branch electronic database, backed up regularly and data should not kept on laptops, personal computers, smartphones.

Any Personal Computer or laptop used by executive committee members to access UK Branch data must be password protected.

Subject Access Requests

All persons who are the subject of personal data held by BSAPRA UK have a right to:

Ask what information the Branch holds about them and why; Ask how to gain access to it;
Be informed how to keep it up to date, how the Branch is meeting its data protection obligations.

Subject Access requests should be made by email or post to the Hon. Secretary.

A charge of £10 may be made, payable before information is provided.

The Hon. Secretary must always verify the identity of the person making a subject access request before handing over any information.

Providing Information

The UK Branch has to ensure that individuals are aware their data is being processed and they understand how the data is being used and how to exercise their rights.

To this end the UK Branch has prepared a Processing and Privacy Notice which will be sent to each successful applicant for membership and be available by request to the Hon Secretary and on the UK Branch web site.

Personal Data Breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example

Personal data breaches can include:

access by an unauthorised third party;
deliberate or accidental action (or inaction) by a controller or processor;
sending personal data to an incorrect recipient;
computing devices containing personal data being lost or stolen;
alteration of personal data without permission; and
loss of availability of personal data.

Any committee member who becomes aware of a possible data breach must inform the IT Officer as soon as possible. The IT officer will investigate the breach and report to the Data Controller (the Executive Committee) who will decide on an appropriate course of action.