GENERAL DATA PROTECTION REGULATIONS - STATEMENT & PRIVACY POLICY

General Statement

Following Brexit, the UK has adopted new laws, to ensure we remain compliant with our EU partners regarding Data Protection issues. The new legislation is known as the UK GDPR January 2021 and follows the EU model with additional sections regarding immigration, law enforcement and the intelligence services. UK GDPR 2021 has enshrined protections for the use of personal data within the UK & European Union. Individuals are becoming increasingly aware about how important it is to ensure that their personal data is kept private. People want control over the information they provide, what happens to that information, who gets to see it, and how long it is kept. If you require any other guidance, please utilise the internet or call the office on **02392 598467** and speak to the data controller or processers.

Personal & Sensitive Data (General)

UK GDPR applies to personal data, which is any information relating to a living individual who can be identified from the data. This identification can be by direct or indirect means, in particular by reference to a specific identifier e.g. name, photograph, work e-mail address, a manager's opinion of an employee in an annual appraisal or an IP address. It also applies to sensitive personal data (defined as 'special categories' of information under UK GDPR) such as genetic data, racial or ethnic origin, political opinion, physical health and sexual life.
Criminal convictions and offences are not included, as separate safeguards apply. UK GDPR is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the United Kingdom. UK GDPR sets out the principles for how data is managed as well as providing rights for the individual.

UK GDPR will be regulated and enforced by the Information Commissioners Office (ICO). If you would like more information you are advised to visit the ICO by clicking on the link below:

Find out more on the Information Commissioner's Website

SB Security Solutions Ltd and Personal / Sensitive Data:

Personal data submitted to or collected by SB Security Solutions Ltd can only be accessed by a restricted number of SB Security staff. These individuals have been provided with training in UK GDPR legislation. They know of the importance of privacy and how to manage employee's data securely and appropriately. SB Security Solutions Ltd will seek your consent, if required by law, to provide access to, or information from, your personal data

We may also have to share your information for the following reasons:

- To abide by any applicable law, regulation, legal process or enforceable governmental request.
- Detect, prevent, or otherwise address fraud, security or technical issues.

All personal and sensitive data is held securely, either by lockable filing cabinets or password protected IT devices.

Functions of the Data Controller & Data Processor:

The Data Controller says how and why any personal data is being processed. The Data Processer acts on the Data Controllers behalf. Within SB Security Solutions Ltd the Data Controller is Francesca Piddington and the Data Processer is Katie Benger. You may contact these individuals by calling **02392 598467** Monday to Friday between 0930 – 1400.

Will your data be shared with third parties?

Your data will not be shared with any third party or used for any commercial or business reason unless it is necessary to comply with legal or regulatory obligations in accordance with the law.

What data is being collected?
We collect personal data about you when you complete your application and vetting forms. The data includes name, home address, phone numbers, email address, bank details, next of kin, medical history, credit checks, vetting details, SIA license details, National Insurance number. This information is required by law to ensure we can pay you for the work you have undertaken for us and determine that you are legally required to carry out work for us.

What is the legal basis for collecting and processing your data?
SB Security Solutions Ltd are required to collect and process your data, in line with the current legislation and regulations, for the purpose of establishing a contract with you. We must also ensure you are legally allowed to work for the company, as well as pay your wages, taxes, NI etc., SB Security Solutions Ltd are also members of the SIA Approved Contractor Scheme (ACS). We must undertake vetting and screening (including credit checking) as required by the scheme in line with the BS:7858 Codes of Practice.

Who is collecting the data and who to contact to amend the data?
Most data collected by SB Security Solutions Ltd, is provided through your application to SB Security Solutions Ltd and vetting forms. The data is usually collected by the Data Controller and Data Processers but may also be collected by your Managers. Should you need to amend or update your data, please contact the Data Controller or Data Processers on **02392 598467.**

How will data be stored?
Personal data will be held in your personnel file and held in a lockable storage facility which can only be accessed by the Data Controller or Data Processers. When you leave the Company, your basic data is transferred to a password protected USB and held in a lockable storage facility.

How long is data held?
Your data will be held while you are employed with SB Security Solutions Ltd. When you leave the Company, your basic information is held for 7 years before it is destroyed, in line with current UK legislation.

How do I access my data?
You have a right to access the personal and sensitive data we hold on you. If you would like to view your data, please contact the head office and obtain a Subject Access Request (SAR) Form. You should fill in the form and return it to the head office to process. Please note that there is a small fee for this service. You may also update, complete, delete (but not critical information required by law) or correct information held on file. To do this you must contact the head office.

How can the data subject raise a complaint?
Contact with our staff or clients, by email, letter or telephone may be recorded. You will be informed if this is the case. Additionally, a briefing note may be made on your file of any conversation held. If you have cause to make a complaint; it is to be made in writing (by letter or email) and sent to the Data Controller at: fran@sbsecuritysolutions.co.uk or to Head Offices address below. An initial reaction and enquiry will be made within 24 hours on a working weekday; with a more formal investigation and response sent within 7 working days.

Unit 4A, Aysgarth Road, Waterlooville, Hampshire. PO7 7UG

Access to Data whilst at the workplace
A copy of the clients Data Protection Policy is available to read and you must not share this, or any information with third parties. This includes any information via emails, World Wide Web (WWW) or any social media devices.

This Policy document is to be read in conjunction with the company "IT Communication & Privacy Policy (QD.12)". Your STAFF HANDBOOK provides additional rules and standards of when access is permitted to data.

- Employees must not use the internet to gain unauthorised access or attempt to gain unauthorised access to computer material or private databases.
- Employees must not use the internet for personal purposes whether during working hours or otherwise, as this may put unnecessary strain on the company's computer network. Internet access is available purely for business use and it should be used for work-related purposes only.
- Internet access may be monitored by the company and the company will conduct an audit of internet usage from time to time. Should any breach of these internet guidelines be discovered, then employees may, in addition to having internet access being withdrawn, be the subject of disciplinary action which, in the case of serious breach, may result in dismissal.
- Employees may not subscribe to any news lists or groups or commit themselves to receiving information from any group or body without first informing their manager. Employees are requested not to view sites which require the downloading of software from the internet, even where this would be free of charge, without the prior approval of their manager. Staff are reminded of the risk of computer viruses.
- Employees must not attempt to download or retrieve illegal, pornographic, liable, sexist, racist, offensive or unlawful material. Attempts to access such material will constitute a disciplinary offence and, in addition to access to the internet being withdrawn, the member of staff may be subject to disciplinary action which may result in dismissal. Information on the internet may not have been placed there with the owner's permission. Therefore, employees must obtain the permission of the copyright owner before transmitting, copying or downloading such information. Where the copyright owner's consent has clearly been given, employees must comply with any terms and conditions stipulated concerning the downloading of such information.
- Information may contain viruses and therefore should not be downloaded from the internet without first obtaining the approval of Sharon Bettesworth and instructions concerning downloading of such information which must be followed. Employees should only download such information which is required for a business purpose. The downloading of information of whatever nature for personal purposes is not permitted.

Review:

This General Statement & Privacy Policy, relating to UK GDPR, will be reviewed annually or if legislation, regulations or company policies are revised.

S Bettesworth

Steve Bettesworth
Managing Director