Bridgegate Security (GB) Limited Privacy Notice.

Part 1. Introduction:

Bridgegate Security (GB) Limited takes data protection very seriously. The use of the Bridgegate Security internet pages, and written forms (e.g. application forms & training documents) may require the submission of personal data, and this data may require further processing. If the processing of personal data is necessary and there is no statutory basis for such processing, we will always obtain written consent from the data subject.

Personal Data processing shall always be in line with the General Data Protection Regulations (GDPR), and in accordance with UK legislation applicable to Bridgegate Security. By means of this privacy notice, we would like to inform the general public why we collect and process personal data, and the rights of the Data Subjects relating to such collection and processing of their data.

Part 2. Definitions:

The Data Protection Notice of Bridgegate Security (GB) Limited is based on the terms used by the European legislator for the adoption of the General Data Protection Regulation but for ease of understanding the following definitions apply.

Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by UK law, the controller or the specific criteria for its nomination may be provided for by that law.

Personal Data: Any information relating to an identified or identifiable natural person (Data Subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number (SIA badge number), location data, an online identifier, or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Subject: Any identified or identifiable natural person, whose personal data is processed, by the controller responsible for the processing.

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recipient: A natural or legal person, public authority, agency or another body, to which personal data is disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with UK law shall not be regarded as recipients (law enforcement agencies); the processing of data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of processing (public office).

Third Party: A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process data.

Restriction of Processing: The protective marking (security classification) of stored personal data with the aim of limiting their processing in the future.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by an automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural persons performance at work, economic situation, health personal preferences, interests, reliability, behaviour, location or movements.

Consent: Consent of the data subject is a freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

Part 3. Name and Address of the Data Controller:

Bridgegate Security (GB) Limited, 541 Woodborough Road, Nottingham, NG3 5FR. Tel: 0115 952 2620, Fax: 0115 952 4696, Email: office@bridgegate-security.co.uk, Web: www.bridgegate-security.co.uk

The Data Control Officer (not data protection officer) for Bridgegate Security (GB) Ltd is: Adam Gidley-Smith, Email: adam.gidley@bridgegate-security.co.uk

Part 4. Cookies:

The internet pages of Bridgegate Security (GB) Ltd use cookies. Cookies are text files that are stored in a computer system via an internet browser. Many internet sites and servers use cookies. Many cookies contain a so-called cookie ID which is a unique identifier of the cookie. It consists of a character string through which internet pages and servers can be assigned to the specific internet browser in which the cookie was stored, this allows visited internet sites and servers to differentiate the individual browser of the data subject from other internet browsers that contain other cookies. A specific internet browser can be recognised and identified using the unique cookie ID. Through the use of cookies, Bridgegate Security (GB) Ltd can provide the users of this website with more user-friendly services that would not be possible without the cookie setting

By means of a cookie, the information and offers on our website can be optimised with the user in mind. Cookies allow us, as previously mentioned, to recognise our website users, the purpose of this recognition is to make it easier for users to utilise our website. Website users that use cookies do not have to enter access data each time the website is accessed because this is taken over by the website, and the cookie is thus stored on the user's computer system. The data subject may, at any time, prevent the setting of cookies through our website by mean of a corresponding setting of the internet

browser used, and may thus permanently deny the setting of cookies. Furthermore, already set cookies may be deleted at any time via an internet browser or other software programs. This is possible in all popular internet browsers. If the data subject deactivates the setting of cookies in the internet browser used, not all functions of our websites will be entirely useable.

Part 5. Reasons/purposes for processing information:

The following is a broad description of the way Bridgegate Security (GB) Ltd processes personal information. To understand how your own personal information is processed you may also need to refer to any personal communications you have received. We process personal information to enable us to comply with UK legislation (e.g. Private Security Industry Act 2001), to conduct background checks on our staff in accordance with BS 7960 2016 Section 5, to promote our services, to maintain our own accounts and records, and to support and manage our employees and contracted service providers.

We collect information relating to the above reasons/purposes from the following sources:

- The Data Subject directly (e.g. from information entered on application forms)
- The Data Subject indirectly (e.g. from your listed references, or through information automatically captured when visiting our web site, such as IP address)
- Publically Available Registers (e.g. SIA website or electoral role)
- Social Media (e.g. Twitter, Linkedin, Facebook)
- Research provided by third parties such as search engines

We process information relating to the above reasons/purposes. This information may include:

- Personal details (including health)
- Business activities of the person whose information we are processing, and their financial details (bankruptcy & bank details)
- Goods and services provided (contracts rendered)
- Educational details
- Employment details (5 year searchable employment history, in line with BS7960)

We also process sensitive classes of information that may include:

- Criminal offences and alleged offences (Rehabilitation of Offenders Act 1974)

We process personal information about our:

- Employees
- Customers & Clients
- Complainants & Enquirers
- Suppliers
- Advisers & other professional experts

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary, we are required to comply with all aspects of the Data Protection Act (DPA), Privacy and Electronic Communications Regulations (PECR), and the EU General Data Protection Regulations (GDPR) as it applies. What follows is a description of the types of

organisations we may need to share some of the personal information we process with, for one or more reasons. Where necessary or required we share information with:

- Business associates, Clients & other professional advisers
- Financial organisations
- Current, past or prospective employers
- Educators and examining bodies
- Suppliers and service advisors
- Law enforcement agencies

Part 6. Rights of the Data Subject.

GDPR affords EU Data Subjects with rights. These rights are summarised below. In order to assert any of these rights the data subject may contact the Data Controller (Bridgegate Security (GB) Ltd) at any time (details in Part 3).

Right of Confirmation: Each data subject shall have the right to obtain from the controller the confirmation as to whether or not personal data concerning them are being processed.

Right of Access: Each data subject shall have the right to obtain from the controller, free information about their personal data stored at any time, and a copy of this information. Furthermore, the data subject shall have a right to obtain information as to whether personal data is transferred to a third country or to an international organisation. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

Right to Rectification: Each data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning themselves. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to Erasure (to be forgotten): Each data subject shall have the right to obtain from the controller the erasure of personal data concerning themselves without undue delay, and the controller shall have an obligation to erase personal data without undue delay where one of the statutory grounds applies, as long as the processing is not necessary.

Right of Restriction of Processing: Each data subject shall have the right to obtain from the controller restriction of processing where a statutory reason applies.

Right to Data Portability: Each data subject shall have the right to receive the personal data concerning them, which was provided to a controller, in a structured, commonly used and machine-readable format.

Right to Object: Each data subject shall have the right to object, on grounds relating to their particular situation, at any time, to the processing of their own personal data.

Automated individual decision making, including profiling: Each data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling.

Right to Withdraw Consent: Where consent forms the basis for processing, data subjects shall have the right to withdraw their consent to the processing of their personal data at any time.

Part 7. Legal basis for processing.

The legal basis for processing shall be where:

- The data subject has given consent to the processing of their personal data for one or more specific purposes (e.g. job application)
- 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 the data subject prior to entering into a contract
- Processing is necessary for compliance with the legal obligation to which the controller is subject (e.g. Private Security Industry Act 2001)
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- 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
- 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 or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

Part 8. The Legitimate Interests pursued by the Controller or by a Third Party.

Where the processing of personal data is based on our legitimate interests, this will be to carry out our business in favour of the well-being of all our employees and the shareholders.

Part 9. Security of Processing.

The Controller, Bridgegate Security (GB) Limited, has implemented technical, physical and organisational measures to ensure personal data stored and processed remains secure. Despite the measures we have taken to secure your information, information sent over the internet, and stored both physically & electronically, can never be 100% secure, and as such we cannot guarantee its absolute security. If you have any questions regarding the security procedures implemented please contact the Data Controller on the details provided in part 3.

Part 10. Personal Data Retention Periods.

Employees: Due to the nature of the business undertaken by Bridgegate Security (GB) Ltd, being that of security work as regulated by the Private Security Industry Act 2001, and the Rehabilitation of Offenders Act 1974, and working to standards set by BS7960, a 5 year checkable work history must be available for anyone working within the security industry. Therefore for our employees, so long as it does not contradict the instructions in any other contract, we will retain information for at least 5 years, from the point of employment termination, before destruction, and longer if there is a legal requirement to do so (e.g. employment tribunal).

Members of the Public: At times we may have cause to obtain personal data from those not in our employment, predominantly through our face to face engagement with the public, and in our efforts to prevent crime and disorder, and the apprehension of those committing criminal offences. This may be in the form of personal details such as name & address, and also CCTV images stored by our clients

(on whose behalf we may be required to review and process). Due to the civil courts of the UK allowing a 3 year period in which to make a civil claim, any such details will be retained for a period of at least 3 years before being securely deleted. Should a claim be brought against the controller, then all data relating to that claim will retained for the duration of the claim process, this may extend beyond 3 years, and will be for as long as is legally required.

Part 11. Contractual obligation of the Data Subject to provide personal data, and the possible consequences of failure to provide such data.

The provision of personal data is partly required by law (e.g. tax regulations) or can also result from contractual provisions (e.g. information on the contractual partner, work history, criminal record etc). Sometimes it may be necessary that in order to conclude a contract, the data subject will be obliged to provide us with personal data, which in turn must be processed by us before the contract can be completed. The non-provision of the personal data in this case would have the consequence that the contract with the data subject would not be concluded.

Part 12. Automated decision-making & profiling.

We do not process any personal data for automatic decision-making or profiling.

Part 13. Transfers.

We do not transfer information overseas. Any information transferred will be done so securely, and in line with UK legislation and all aspects of GDPR.

Part 14. Data protection for Employment & Recruitment Procedures.

The data controller shall collect and process the personal data of applicants for the purpose of the processing of the application procedure. The processing may also be carried out electronically. This is the case, in particular, if an applicant submits corresponding application documents by e-mail or by means of a web form, to the controller. Any such electronically received documents shall be deemed as 'signed' by the applicant by way of the electronically traceable e-mail 'thread'. If the data controller concludes an employment contract with an applicant, the submitted data will be stored for the purpose of processing the employment relationship in compliance with legal requirements. If no employment contract is concluded with the applicant by the controller, the application documents shall be automatically erased two months after notification of the refusal decision, provided that no other legitimate interests of the controller are opposed to the erasure. Other legitimate interests could be complying with UK legislation such as the Equality Act 2010.

Part 15. General.

You may not transfer any of your rights under this privacy notice to any other person. We may transfer our rights under this privacy notice where we reasonably believe your rights will not be affected, (such as in event of a change of ownership).

If any court or competent judiciary authority finds that any provision of this privacy notice (or part thereof) is invalid, illegal or unenforceable, that provision or part-provision will, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of this privacy notice will not be affected.

Unless otherwise agreed, no delay, act or omission by a party in exercising any right or remedy will be deemed a waiver of that, or any other, right or remedy.

This notice will be governed by and interpreted according to the law of England & Wales. All disputes arising under the notice will be subject to the exclusive jurisdiction of the English & Welsh courts.

Part 16. Updates & Changes.

This notice was last updated on the 23rd May 2018. We may change this policy by updating this page to reflect changes in the law or our privacy practices. However, we will not use your personal data in any new ways without your consent.