Scannet Hardware, Software and Services Agreement

INFORMATION SHARING AGREEMENT

This Information Sharing Agreement ("ISA") is supplemental to the Scannet: Hardware, Software and Services Agreement and will apply in addition to the Agreement where a Client has selected to access the Scannet Shared Alert System and use the data contained within the Scannet Data Repository.

1. INTRODUCTION

1.1 This ISA has been drawn up under the umbrella of best practice guidance from the National Pubwatch, Thames Valley Police, Metropolitan Police, Hampshire Police and Cambridgeshire Police. Collectively these sources have contributed to the core information sharing principles and obligations set out in this ISA.

1.2 The Licensing Act 2003 states that licensed businesses and their staff are legally obliged to ensure that they do not serve alcohol to anyone under the age of 18 years. Licensed businesses are also required by law to prevent crime and disorder, prevent public nuisance and ensure the safety of those using their premises. To assist licensed businesses to comply with these legal obligations, this ISA is established between Scannet Users who wish to access and use the Scannet Shared Alert System to support the sharing of selected information between them in accordance with the Privacy and Data Protection Requirements.

1.3 Any definition not provided in this ISA shall have the same meaning as set out elsewhere in the Agreement. In this ISA the following additional definitions shall apply:

"Agreement" means the Order Form and Scannet: Hardware, Software and Services Agreement entered into between GBG and the Client.

"Customer" means a member of the public who wishes to gain entry to premises operated by a Scannet User.

"Network Alert" means a digital communication describing an alleged incident that took place at the premises of an Alert Sharer who has chosen to share these details with other Alert Sharers.

"Network Alert Originator" means the Alert Sharer who creates a Network Alert**.**

"Network Alert Recipient" means an Alert Sharer in receipt of a Network Alert.

"Network Alert Subject" means the individual Customer involved in the incident who is the subject of the Network Alert.

"Scannet" means the Hardware, Software and Services which collectively perform identity document scanning and age verification in accordance with the terms of the Agreement.

"Scannet Users" means any Client who accesses the Scannet Shared Alert System in accordance with their Agreement with GBG and this ISA.

"Super Administrator" means a manager within the Alert Sharer's business that is granted access to the Scannet server's web portal and who is capable of deleting a Network Alert or amending the alert distribution.

1.4 All Alert Sharers are inherently Scannet Users but, unless they are signatories to this ISA, Scannet Users are not automatically Alert Sharers and will not have access to the Scannet Data Repository. For clarity, in this ISA the use of the term "Alert Sharer" will include reference to an Alert Sharer and their Permitted Users.

1.5 The Scannet Shared Alert System allows Alert Sharers to form their own sub-groups within its environment. However, these sub-groups are governed by their own rules, procedures and information sharing arrangements subject to the terms of this ISA.

1.6 This ISA supplements the Agreement and sets out binding obligations owed by Alert Sharers.

2. POLICY STATEMENTS AND PURPOSE

2.1 To help licenced businesses comply with their obligations under the Licensing Act, information processed in an individual Scannet system may be shared between Alert Sharers through transmission to the Scannet Data Repository from which certain details are made available to other Alert Sharers.

2.2 Scannet is a computer system which takes a scanned copy of an identity document volunteered by a Customer. From this scanned copy, Scannet checks the age of the Customer and, if the Scannet User is also an Alert Sharer, whether a Network Alert has been shared with the Scannet Data Repository in relation to that Customer by another Alert Sharer.

3. SCANNET IS VOLUNTARY

3.1 GBG does not oblige Alert Sharers to scan Customer IDs through Scannet. Similarly, GBG does not oblige Customers of Alert Sharers to provide their IDs for scanning by Scannet.

3.2 Where a Customer allows an Alert Sharer to scan their ID, the Alert Sharer shall use the information acquired from the ID for the following reasons only:

(a) Personal safety;
(b) To create a log of customers on the premises at a given time;
(c) To assist the police and/or local authorities on request therefrom for access to relevant information;
(d) To create a Network Alert to be shared with other Alert Sharers, in the event that a Network Alert Subject has behaved in a way which may threaten the Alert Sharer's licence and/ or the alert would help Alert Sharers fulfil any of the main provisions of the Licensing Act 2003; and
(e) For statistical analysis.

4. DATA PROTECTION

4.1 The Agreement sets out responsibilities of Scannet Users which include obligations to comply with all Privacy and Data Protection Requirements. Each Scannet User and Alert Sharer warrants that it is a Controller in relation to all Personal Data gathered using Scannet including any Personal Data subsequently shared via the Scannet Shared Alert System.

4.2 In order to obtain, use or disclose Personal Data of a Customer, each Scannet User and Alert Sharer acknowledges and accepts that it is solely responsible for ensuring that the Customer is provided with, or has made readily available to it a copy of the Scannet User's Data Protection Notice containing: the identity of the Scannet User; the purpose, or purposes, for which any data or information gathered using Scannet will be processed; and further information necessary, in the specific circumstances, to enable the processing in respect of each Data Subject to be fair.

4.3 GBG provides services to Alert Sharers which include the hosting of the Scannet Data Repository. By entering into this ISA, each Alert Sharer hereby appoints GBG to provide such services and act as Data Processor and Data Co-Controller of any Personal Data which is shared via the Scannet Shared Alert System and stored in the Scannet Data Repository. The Data Responsibility Table in Appendix 1 shows what duties apply to which party.

4.4 GBG and Alert Sharer each warrant and undertake to the other that it shall at all times:

(a) Implement and maintain appropriate technical and organisational security measures against unauthorised or unlawful processing of Personal Data shared via the Scannet Shared Alert System and stored in the Scannet Data Repository against accidental loss or destruction of Personal Data or damage to the Personal Data in accordance with all Privacy and Data Protection Requirements;
(b) Co-operate in a timely manner with the other Party to enable the other Party to comply with any lawful exercise of rights by a Data Subject in respect of any Personal Data processed by the other Party in accordance with this ISA;
(c) Promptly notify the other Party in writing should they become aware of any breach or potential breach of the Privacy and Data Protection Requirements which is relevant to this ISA;
(d) Promptly notify, where relevant, the other Party of any assessment, enquiry, notice or investigation by the UK Information Commissioner or any equivalent supervisory authority in any other jurisdiction which might involve all or part of the Personal Data and comply with the same including without limitation, providing all reasonable information and assistance requested by the other Party within the time scale reasonably specified by the other Party in each case.

4.5 GBG shall only process the data stored in the Scannet Data Repository in accordance with the provisions of this ISA and the Agreement in order to make the Scannet Shared Alert System available to Alert Sharers and shall not access or use Personal Data relating to any individual Customer of an Alert Sharer for any purpose save only that GBG may remove Network Alerts transmitted by any Alert Sharer where:

(a) The Network Alert Originator has ceased trading, ceased to operate or otherwise become uncontactable; or
(b) Pursuant to the termination provisions under this ISA.

4.6 In accordance with the Privacy and Data Protection Requirements all UK based Controllers (i.e. UK based Scannet Users and Alert Sharers) must register with the Information Commissioner's Office and to maintain their registration until they cease to be Controllers. All Controllers are individually responsible for complying with the Privacy and Data Protection Requirements and for developing their own data protection policies. These policies should include a data retention schedule and a clear protocol for responding to the rights of a Data Subject as prescribed by law. Alert Sharers who form groups may want to develop their own group data protection policies as well. Any questions about the rights and responsibilities of a Controller should be directed to the Information Commissioners Office.

4.7 In the event of a change to any Privacy and Data Protection Requirements or best practice guidance during the term of the Agreement, GBG reserves the right upon written notice to amend the terms of this ISA to the extent necessary to ensure continuing compliance of either Party with any such change.

5. NETWORK ALERTS

5.1 Network Alerts are transmitted to the Scannet Data Repository by the Network Alert Originator. Customers attending venues operated by Scannet Users may be requested to volunteer their ID for scanning. When a Customer's ID is scanned at an Alert Sharer's venue, it is automatically compared with the IDs stored within the Scannet Data Repository.

5.2 When a Customer ID that is presented to an Alert Sharer matches a Network Alert stored on the Scannet Data Repository certain details of that Network Alert are made available to the Alert Sharer (now a Network Alert Recipient). The information on the Customer ID is used to decrypt and display the Network Alert information therefore this information is only made available upon the presentation of the matching Customer ID.

5.3 Scannet will display an image of the Network Alert Subject side by side with an image of the face contained on the present Customer's ID document so the Network Alert Recipient can make an informed decision about whether the displayed faces match.

5.4 If the Network Alert Recipient using their own discretion indicates that they believe that the two images are of the same person, Scannet will then display the question "Do you want to see the alert?" If the Network Alert Recipient selects an affirmative response, the Network Alert Recipient is presented with a screen which displays the:

(a) Code of the alleged offence;
(b) Date of the Network Alert;
(c) Expiration date of the Network Alert;
(d) Name of the Network Alert Originator; and
(e) Address of the Network Alert Originator.

5.5 Network Alert Recipients may use the details contained in a received Network Alert in accordance with their individual license conditions and admission policies to decide whether the Customer should be allowed entry. At this stage, the Network Alert Recipient can speak with the Customer and can, considering their responsibilities under the Licensing Act 2003 (and/or any conditions attached to the venue's license under the Licensing Act 2003), decide whether to allow the Customer entrance to their premises.

5.6 The nature of the alleged incident will be specified in the Network Alert as a code which will typically be related to undesirable conduct of some kind including potential criminal, unsafe or nuisance behaviour (e.g. swearing, spitting, abusive or aggressive behaviour). This may also include particular behaviours or activities inconsistent with the license conditions or admission policies applicable to the Network Alert Originator.

5.7 The Parties acknowledge and accept that a Network Alert is NOT a ban. A Network Alert is an allegation made by the Network Alert Originator. A Network Alert should not be treated by a Network Alert Recipient as an automated decision to bar a Network Alert Subject from their premises. Instead, a Network Alert provides information which allows a Network Alert Recipient to consider the situation, have a discussion with the Network Alert Subject and make an informed decision about whether to admit the person to their premises.

5.8 Scannet uses secure encrypted methods for the transmission of Network Alerts to the Scannet Data Repository and the sharing of Network Alerts with Network Alert Recipients. A Network Alert which is shared with a Network Alert Recipient comprises only basic data elements. These are regularly synchronized with the Scannet Data Repository so that all Network Alerts are stored on the Scannet User's Scannet system.

5.9 Scannet is not a searchable database of Network Alert Subjects as the Network Alerts are delivered in an encrypted format which can only be decrypted by the Network Alert Subject's unique identity when presented to a Scannet machine by an Alert Sharer. The information shared consists of a photograph of the Network Alert Subject, the alert code and the date of the alleged offence. (The technology underpinning this process is described in UK Patent Application No. EP 2 988 291 A1).

6. WARRANTIES AND OBLIGATIONS

6.1 The Alert Sharer warrants that it shall comply with all applicable legislation, instructions and guidelines issued by regulatory authorities, relevant licences and any other codes of practice which apply to the Alert Sharer and its use of the Scannet Shared Alert System including those which relate to the provision of a Network Alert. In particular the Alert Sharer:

(a) shall ensure all data shared as part of a Network Alert will be supplied using reasonable care and skill and in accordance with the terms of this ISA and the Agreement; and

(b) will not supply information which is false or misleading, save where any error or omission arises from the adoption in good faith of information provided by a source on which it is reasonable for the Alert Sharer to rely and despite the Alert Sharer's exercise of all reasonable care and diligence.

6.2 As a Network Alert is not a ban, Network Alert Recipients should not maintain a default position of refusing entry to any Customer found to match a Network Alert Subject. Instead, Network Alert Recipients should use the information contained in the relevant Network Alert as a basis for a possible conversation with the person and then make an informed decision whether to allow the Customer entry.

7. GUIDELINES TO BE FOLLOWED BY ALERT SHARERS

7.1 Generating an Alert

7.1.1 The content of a Network Alert will vary according to the circumstances of the alleged incident. Similarly, the decision about whether or not to create a Network Alert for a given alleged incident and the specific details to be included therein, is at the sole discretion of the individual Network Alert Originator. The purpose of a Network Alert is to provide sufficient information regarding an alleged incident to other Alert Sharers to enable informed decision-making regarding the admittance of a Network Alert Subject to their premises.

7.1.2 To support compliance with statutory obligations under the Licensing Act 2003, all Network Alert's created and shared using the Scannet Shared Alert System should contain the:

(a) alert code setting out the reason for the Network Alert;
(b) creation date of the Network Alert;
(c) identity of the Network Alert Originator; and
(d) duration of the Network Alert (in accordance with individual policies).

7.1.3 Scannet can be customised to email the Super Administrator of the Network Alert Originator when a Network Alert is created, thereby establishing a complete audit trail of the Network Alerts created by the relevant Alert Sharer.

7.1.4 For reference, "the alleged commission…of any offence" is considered by the Privacy and Data Protection Requirements to be "sensitive personal data" which requires more careful processing and should be taken into account by the Scannet User.

7.2 Privacy Notice

7.2.1 Personal Data acquired from a presented Customer ID should be volunteered to Scannet Users by Customers in accordance with the "Information Commissioner's Data Protection Good Practice Notice for the Use of ID Scanning Devices in Pubs and Clubs".

7.2.2 As set out in the Agreement, Alert Sharers must:

(a) display an appropriate Data Protection Notice at the points of entry to participating venues;
(b) post a copy of such Data Protection Notice on its website in a publically accessible place; and
(c) supply door staff with Data Protection Notice cards to distribute to Customers on entry to participating venues;

describing the operation of Scannet, the Scannet Shared Alert System and the processing of Personal Data which takes place at the point of entry to participating venues in accordance with the Good Practice Guidance provided by GBG.

7.2.3 All Permitted Users (including door staff and management) must read and understand the Data Protection Notices and the Information Commissioner's Good Practice Note for the Use of ID Scanning Devices in Pubs and Clubs.

7.3 Information to be Shared

7.3.1 There is no searchable database of the names of Network Alert Subjects.

7.3.2 Details of a Network Alert Subject are only shared with an Alert Sharer when a statistical match is achieved between the details of a Customer newly arrived at the premises of the Alert Sharer and those of the relevant Network Alert Subject.

7.3.3 Only segments of an individual's Personal Data (e.g. 3rd and 4th letter of first name, 2nd, 6th and 8th letters of address, last two digits of year of birth and photograph) are shared via the Scannet Shared Alert System. It is not possible to identify an individual from the shared segments of data. The comparison between the shared data segments and the details of the new Customer is inherently statistical in nature. Further information about the Network Alert Subject is only revealed to the Alert Sharer on completion of the steps set out in Clause 5.

7.4 How Will Personal Data Be Transferred?

7.4.1 Personal Data is encrypted when it is being transferred and when it is at rest on all machines, including the Scannet Data Repository. While it hosts and stores the Scannet Data Repository, GBG does not have readable access to Network Alerts or any other Personal Data collected by Alert Sharers relating to Network Alert Subjects. Using the Scannet Data Repository, Alert Sharers share and receive Personal Data amongst each other and, acting as Network Alert Originators, control what information is transmitted to the Scannet Data Repository for sharing with other Alert Sharers.

7.4.2 Unless required or allowed to under specific legislation or decree, Alert Sharers must not transfer information created or received through the Scannet Data Repository to any third party (i.e. any person other than another Alert Sharer or, for hosting and service provision purposes, GBG) or outside of the EEA.

7.5 Administrative Guidelines

7.5.1 The Alert Sharer is responsible for the acts and omissions of all Permitted Users and is liable for any failure by any such individual to perform or observe the terms and conditions of this ISA and the Agreement.

7.5.2 Alert Sharers must ensure that each Permitted User has their own unique login profile. This ensures that each venue is able to maintain an audit log of all users and actions.

7.5.3 Alert Sharers must ensure that use of the Scannet Shared Alert System is hierarchically restricted. More specifically, Alert Sharers must ensure that specified types of Permitted Users can only access correct levels of information. For example, door staff should be provided with limited access to the Scannet Shared Alert System, so that they are permitted only to receive, process and create alerts and not delete them.

7.5.4 Alert Sharers will designate at least one individual at management level as a Super Administrator who shall be permitted access to the server's web portal (for example, a Super Administrator may be a General Manager or a Director of the Alert Sharer). The Super Administrator will be the only member of staff in the Alert Sharer capable of deleting an alert or amending the alert distribution. Depending on the organisational structure of a given Alert Sharer, "supervisor" and "administrator" access level may be accorded to a junior manager and senior manager respectively.

7.5.5 Alert Sharers will ensure that all Permitted Users, and most especially the designated Super Administrator, receive appropriate information security and data protection training.

7.6 Ensuring Data Quality

7.6.1 All Alert Sharers sharing data under this ISA are solely responsible for the data that they are gathering and sharing and their compliance with the Privacy and Data Protection Requirements.

7.6.2 Before sharing a Network Alert, a Network Alert Originator should check that the information contained in the Network Alert is accurate and up to date. Particular care should be taken as the Network Alert is likely to contain sensitive data which could harm or cause distress to the Network Alert Subject were it inaccurate.

7.6.3 If a complaint is received about the Personal Data which forms the basis of a Network Alert, the Network Alert Originator shall investigate the complaint in accordance with their internal policies and if necessary freeze processing while the Network Alert is under investigation, but in each case reasonable steps must be taken to ensure the accuracy of the allegation made in the Network Alert. Where appropriate the Network Alert Originator shall:

(a) update the relevant Network Alert;
(b) delete the relevant Network Alert; or
(c) annotate the Network Alert to record that the Network Alert Subject considers the allegation to be inaccurate.

7.7 Information Use, Review, Retention and Deletion

7.7.1 Alert Sharers shall ensure that Personal Data shared under the ISA will only be used for the purpose of providing information about an alleged incident sufficient to enable informed decision-making by the Network Alert Recipients regarding the admittance of a Customer to further venues; thereby helping Alert Sharers to comply with their statutory obligations under the Licensing Act 2003. Personal Data must not be shared between Alert Sharers for any other purpose.

7.7.2 In accordance with Principle 5 GDPR Personal Data should only be kept for as long as deemed necessary by the Controller. Alert Sharers should establish their own internal guidelines for the retention of Personal Data including all data gathered via Scannet and all Network Alerts for which they are the Network Alert Originator.

7.7.3 For clarity, in accordance with the principles of the Privacy and Data Protection Requirements, a Network Alert Originator must ensure that Network Alerts are accurate, up-to-date, adequate and not excessive (amongst other principles). Alert Sharers are responsible for their own data protection policies, however, it has been recommended that Network Alerts are reviewed by Network Alert Originators at least every three months.

7.7.4 The deletion of Network Alerts does not indicate the deletion of a Customer's ID profile on your Scannet system.

8. MISCELLANEOUS PROVISIONS

8.1 Roles and Responsibilities

8.1.1 The Alert Sharer will allow GBG to add Network Alerts to the Scannet Data Repository and share the Network Alerts with other Alert Sharers.

8.1.2 GBG shall provide the Scannet Shared Alert System in accordance with the terms of this ISA and the Agreement.

8.1.3 The Alert Sharer acknowledges and accepts that occasionally GBG, in providing the Scannet Shared Alert System, may be required to:

(a) change the technical specification of the Scannet Shared Alert System for operational reasons, however, GBG will ensure that any change to the technical specification does not materially reduce or detrimentally impact the performance of the Scannet Shared Alert System;
(b) give the Alert Sharer instructions which it reasonably believes are necessary to enhance or maintain the quality of any Scannet Shared Alert System provided by GBG and GBG shall not be responsible for any errors in the Scannet Shared Alert System resulting from the Client's non-compliance with such instructions; and
(c) suspend the Scannet Shared Alert System for operational reasons such as repair, maintenance or improvement or because of an emergency, in which case GBG will give the Alert Sharer as much online, written or oral notice as possible and shall ensure that the Scannet Shared Alert System is restored as soon as possible following suspension.

8.1.4 The Scannet Shared Alert System is provided solely for the Alert Sharer's own internal use. The Alert Sharer must not resell or attempt to resell the Scannet Shared Alert System to any third party.

8.1.5 Information shared between Alert Sharers must not be disclosed to any third party without the written consent of the Network Alert Originator. For the purposes of this ISA, approval for such sharing lies with the Super Administrator of the Network Alert Originator.

8.1.6 Each Alert Sharer agrees and undertakes to all other Alert Sharers that it shall comply with its legal obligations relating to the rights of a Data Subject and any subject access request made by any and all Network Alert Subjects.

8.1.7 Each Alert Sharer agrees and undertakes to indemnify the other Alert Sharers and GBG in respect of any fines, proceedings, costs, claims, liabilities or expenses suffered or incurred by any indemnified party which is attributable to any breach by the Alert Sharer of any provision of this ISA.

8.2 Intellectual Property Rights

8.2.1 The Scannet Shared Alert System is protected by Intellectual Property Rights. The Alert Sharer must not copy, store, adapt, modify, transmit or distribute the Scannet Shared Alert System except to Permitted Users or permit anyone else to do the same.

8.2.2 The Alert Sharer acknowledges that all Intellectual Property Rights in the Scannet Shared Alert System shall belong and shall continue to belong to GBG. GBG grants a licence to the Alert User to use the Scannet Shared Alert System under the terms of this ISA.

8.2.3 Subject to clause 8.2.2, GBG acknowledges all Intellectual Property Rights in a Network Alert belong and shall continue to belong to the Network Alert Originator. The Network Alert Originator grants to GBG a transferable, sub-licensable, non-exclusive, royalty free licence to use, disclose and copy the Network Alert to enable GBG to provide the Scannet Shared Alert System and carry out its obligations under this ISA.

8.2.4 The Alert Sharer warrants that: (a) it will not use or exploit the Intellectual Property Rights in the Scannet Shared Alert System or permit others to use or (b) exploit the Intellectual Property Rights in the Scannet Shared Alert System outside of the terms of the licence granted to the Alert Sharer in this ISA.

8.2.5 If any third party makes or threatens to make a claim against GBG or the Alert Sharer that the use of the Scannet Shared Alert System infringes any third party's Intellectual Property Rights, GBG shall be entitled to do one or more of the following:

(a) suspend any part of the Scannet Shared Alert System that is subject to the infringement claim made by the third party;
(b) modify the Scannet Shared Alert System, so as to avoid any alleged infringement, provided that the modification does not materially affect the performance of the Scannet Shared Alert System; and/or
(c) terminate the ISA upon written notice to the Alert Sharer.

8.3 Liability

8.3.1 Neither Party excludes or limits its liability for death or personal injury resulting from its negligence, fraudulent misrepresentation or any other type of liability that cannot by law be excluded or limited.

8.3.2 Neither Party excludes or limits its liability in respect under clauses 3, 4, 6, 7, 8.1 and 8.2 of this ISA.

8.3.3 Subject to clauses 8.3.1 and 8.3.2, each Party's aggregate liability to the other Party under or in connection with this ISA, whether such liability arises in contract, tort (including, without limitation, negligence) misrepresentation or otherwise, shall be limited to £5,000.

8.3.4 Subject to clauses 8.3.1 and 8.3.2, neither Party shall be liable for loss of profits, business or anticipated savings, loss or destruction of data, loss of use of data, loss of reputation, loss of goodwill, any special, indirect or consequential loss or damage.

8.3.5 The Alert Sharer agrees that, except as expressly set out in this ISA, all warranties, conditions and other terms relating to the Scannet Shared Alert System whether express or implied by law, custom or otherwise are, to the fullest extent permitted by law, excluded from this ISA.

8.3.6 The Parties acknowledge that damages alone may not be an adequate remedy for a breach by the other Party of 3, 4, 6, 7, 8.1 and 8.2 of this ISA. Accordingly, without prejudice to any other rights and remedies it may have, the injured Party shall be entitled to seek specific performance and/or injunctive or other equitable relief.

8.4 Governing Law and Jurisdiction

8.4.1 By entering into this ISA, the Parties warrant that they each have the right, authority and capacity to enter into and be bound by the terms and conditions of this ISA and that they agree to be bound by these.

8.4.2 This ISA and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed and construed in accordance with the laws of England and both Parties submit to the exclusive jurisdiction of the English Courts, save that GBG may elect to bring proceedings against the Alert Sharer in the courts of any jurisdiction where the Alert Sharer or any of the Alert Sharer's property or assets may be found or located.

Scannet Hardware, Software and Services Agreement

APPENDIX 1 – DATA RESPONSIBILITY TABLES

THE BELOW TABLES ARE DESIGNED TO PROVIDE CLEAR ACCOUNTABILITY FOR EACH PARTY

Responsibility	Scannet Client	GBG
Data Collection	ID document collected direct from the subject, alert code and duration of alert and any comments added by the Scannet operator on behalf of the Client	GBG is unable to influence the original data collected.
Notification to Data Subject	This responsibility sits with the Client with their privacy notice, process and procedures for creating a Shared Alert	GBG has no control over setting Shared Alerts.
Purpose Limitation - Is personal data only used for the purposes for which it was originally collected?	This responsibility sits with the Client.	GBG has no control over data usage.
Data minimisation – Is the personal data limited to what is necessary for the purposes for which it is processed?	The Client should not scan additional documents that are not required.	GBG has no control over what documents are scanned.
Accuracy – Are policies and training in place to ensure personal data are checked and where inaccurate are rectified without delay?	This responsibility sits with the Client.	GBG has no control over the accuracy of their data.
Storage limitation (retention) – Do privacy policies incorporate information on retention? Are these procedures in place for arching and destruction of data?	This responsibility sits with the Client.	GBG has no control over how long data are retained. GBG can influence the retention period with the suggested system retention period and shared alert periods
Integrity and confidentiality	Appropriate technical and security measures defined by the Client in order to protect the data within their environment.	Appropriate technical and security measures are used to protect the data defined by GBG are used to protect the data within the GBG environment.
Accountability	Demonstrate compliance with data protection principles.	Demonstrate compliance with data protection principles.
Access to personal data - procedure for handlings subject access requests.	The Client will respond to the data subject advising them on the data, alert code, duration of alert and notes held.	GBG does not normally hold personal data on behalf of clients but will respond to the data subject advising them on any data and notes held if data has been shared.
Access to personal data – individuals are provided with a mechanism to request access to information about them.	This responsibility sits with the Client.	GBG has a process for handling of Subject Access Requests.
Access to personal data - Data Controller must respond to SARs within one month	Yes	Yes
Erasure & rectification – individuals are informed of their right to demand erasure and rectification of personal information held about them.	The Client will assess the data subject's request and reply accordingly. In some cases, it will not be appropriate to restrict or to stop processing or delete data.	GBG is unable to influence the original data collected but will contact the Client.
Erasure and rectification – controls and formal procedures in place to allow personal data to be erased or blocked.	The Client will assess the data subject's request and act accordingly. In some cases, it will not be appropriate to restrict or to stop processing or delete data.	GBG is unable to influence the original data collected but will contact the Client.
Right to object – individuals are told about their right to object to certain types of processing	The Client will assess the data subject's request and reply accordingly. In some cases, it will not be appropriate to restrict or to stop processing or delete data.	GBG will assess the data subject's request and reply accordingly.
Profiling and automated processing	No profiling.	No profiling.

		GBG Scannet			
Functions	**Client**	**Processor for Client**	**Controller**	**Joint Controller**	**Decision Rationale**
Collection of personal data	Controller	Y	N	N	Data collection is performed by the Client.

Sharing Alerts with other Clients	Controller	Y	N	N	Data collection is performed by the Client and radius of alerts is set by Client.
Shared Alerts Period	Controller	Y	N	N	The length of a shared alert is set by the Client but GBG provide a choice of time periods for the shared alert in the software.
Shared Alerts data held	Controller	Y	N	Y	GBG provide a range of alert types. When a venue closes or stops using Scannet, any existing alerts will be retained within the shared alerts system until they expire.
Responding to Subject Access Requests	Controller	Y	N	N	As Processor, GBG will pass on all requests to the Client.