PRODUCT SCHEDULE

GBG GO – COMPLIANCE PLATFORM

The Compliance Platform Service is provided by GBG's wholly owned Group Company, Acuant Inc ("Acuant"). The platform is hosted in Germany, but for some services an API call out is made to the US. Where a data transfer is made, this is detailed in the Additional Terms.

1 DEFINITIONS AND INTERPRETATION

1.1 In this Product Schedule the following definitions shall apply in addition to those contained within the GBG GO Product Terms and the General Terms:

"**Compliance Platform Service**" mean delivery of Identity Fraud Assement and/or PEP's & Sanctions.

"Identity Fraud Assessment" means the part of the Compliance Platform Service which performs identity validation by evaluating different/additional datasets: device fingerprint (i.e. a device ID that describes the type of device being used), IP address and entity link analysis (i.e. match against the data contained in eDNA from other customers) in order to evaluate the level of risk associated with an individual. Relevant Datasets: Device Fingerprint Dataset ID 201764, IP Risks & Insights Dataset ID 201765, Document Verification (Manual) Dataset ID 201766, Face Match (Manual) Dataset ID 201767, Adverse Media Diligent Dataset ID 201768.

"PEP's & Sanctions" means the service that helps verify if an individual or entity is a politically exposed person or sanctioned individual. Relevant Dataset: On Boarding Sanctions & PEPS Dataset ID 201763.

1.2 The headings in these Product Terms do not affect its interpretation.

2 DATA PROTECTION: COMPLIANCE PLATFORM

2.1 In delivering the Compliance Platform Service:

a) the Customer is a controller of the Customer Data. To the extent that Acuant processes the Customer Data received from GBG to provide Compliance Platform Service, it shall do so as a separate and independent controller.

b) Acuant is a controller of the Supplier Data that it uses to supply the Service and Results to the Customer. The Customer shall act as a separate and independent controller of the Results, which it shall use solely for the Customer Use Case

c) GBG shall act as the Customer's processor.

2.2 In acting as a controller, as described in clause 2.1 a) & b) above, both the Customer and Acuant shall comply with clause 9 of the General Terms. In this respect, any references to GBG shall be referring to Acuant. The Customer's and Acuant's responsibilities in their capacity of independent controllers are set out in Annex 1 to this Product Schedule.

2.3 In acting as the Customer's processor, as described in clause 2.1 c), GBG shall comply with clause 8 of the GBG GO Product Terms.

2.4 **Data Retention**: Customer may exercise an option to have Acuant retain the Customer Data the Customer has sent to GBG, as well as the processing activities conducted on such data, after termination of the Agreement. Acuant may retain Customer Data along with other data attributes provided by other Customer's clients to match transaction information for the purpose of determining fraud, reputation, and identity as it relates to transactions in the eDNA Digital Identity Engine or to improve or develop its products for commercial purpose. Data is retained within eDNA Digital Identity Engine for up to 10 years.

3 EDNA DIGITAL IDENTITY ENGINE

3.1 In providing the Compliance Platform Service, Customer understands and agrees that Customer Data may be transferred into Acuant's data consortium network, "**eDNA Digital Identity Engine**" to assist in the detection and prevention of fraud for third party customers. All Customer Data shall be pseudonymised, hashed, and encrypted. Whilst this personal data may be used to provide services for Acuant's other Customers, it is only utilised to derive and provide a fraud risk score on their behalf and Customer Data in eDNA is not provided or transferred to any third parties.

ANNEX 1 - RESPONSIBILITY TABLE FOR CONTROLLER PERSONAL DATA

Responsibility	Acuant	Customer
Data subject personal data collection	No control over what data is collected from data subjects.	The Customer decides what personal data to collect from the data subjects.
Source of personal data and information provided to the data subject	Acuant is unable to influence the personal data collected, but must consider information provided about the data subject through its separate interaction with the data subject (i.e. when monitoring instances of data subjects personal data being processed via the eDNA Digital Identity Engine).	Customer is responsible for providing appropriate information to the data subject in accordance with Applicable Data Protection Law.
Notification to Data subject	Acuant must consider Article 14 of GDPR or equivalent of Applicable Data Protection Law.	The Customer informs the data subject the data will be supplied to third parties for the Customer Use Case, provides all required transparent disclosures via a privacy notice and/or notice on collection, and obtains any necessary consents that are required under applicable law.
Accuracy	If a data subject questions the accuracy of their data, GBG will pass the details of the request to the Customer for review and rectification if required.	The responsibility to update a record at source sits with the Customer.
Storage limitation (retention)	Acuant has its own independent retention policy for personal data as set out in its privacy policy	Customer has its own independent retention policy for the personal data as set out in its privacy policy.
Access to personal data – single point of contact regarding all data subject rights requests and procedure for handling subject access requests	Acuant email: compliance@gbgplc.com. This email will be monitored by Acuant Inc.'s parent company GBG to facilitate requests from the Customer regarding individual rights.	Customer email as outlined on order form This email will be monitored by the Customer to facilitate requests from GBG regarding individual rights.
	Following notification from the Customer, GBG or Acuant Inc will respond directly to the data subject in accordance with Applicable Data Protection Law and promptly inform the Customer of any action taken.	The Customer will respond to data subject access requests in accordance with Applicable Data Protection Law. Where appropriate, this will include informing the data subject that GBG is a recipient or a category of recipient to whom the data is disclosed. Where appropriate (for example, in order to provide a single contact point for individuals who wish to exercise their rights), Customer

Responsibility	Acuant	Customer
		will contact GBG in relation to the data subject access request.
Erasure, rectification, restriction and notification – controls and procedures to erase, rectify or restrict personal data (as may be required) and discharge notification requirements	Acuant Inc will action and respond to such requests (where received directly, or from the Customer) in accordance with Applicable Data Protection Law.	Customer will action and respond to such requests in accordance with Applicable Data Protection Law.
Right to object – procedures to respond to a data subject's right to object	Acuant will assess the data subject's request in accordance with Applicable Data Protection Law.	Customer will assess the data subject's request in accordance with Applicable Data Protection Law.
Data Breach Notifications	Acuant agrees to notify the Customer pursuant to clause 9 of the General Terms.	Customer agrees to notify GBG pursuant to clause 9 of the General Terms: compliance@gbgplc.com, security@gbgplc.com