

GBG GO – IDV

The IDV Service is provided by GBG’s 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.

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:

“IDV Service” means the provision of AssureID Connect, Facematch and/or Passive Liveness.

“AssureID” means the Services whereby Acuant processes the markers on ID documents (e.g., stamps, font, positioning) in order to match against its own document library of ID documents, in order to authenticate the ID document. Relevant Dataset: Document Verification (Auto) Dataset ID 201759.

“Facematch” means the Services whereby Acuant compares a data subject’s selfie image to the photo from their ID document to verify if the individual in the selfie matches the individual in the ID document by processing biometric data. Relevant Datasets: Document Verification+Face Match Dataset ID 201760.

“Passive Liveness” means the Services whereby Acuant provides liveness detection to ensure selfie picture is of a live person and is not an image of a video or photo. Relevant Datasets: Document Verification + Face Match + Liveness Dataset ID 201761, Document Verification + Liveness 201762.

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

2. DATA PROTECTION: IDV

2.1 In delivering the IDV Service:

- a) the Customer is a controller of the Customer Data that it supplies to GBG, and shall comply with clause 9 of the General Terms.
- b) GBG shall act as a processor and Acuant shall act as an authorised sub-processor for the delivery of the IDV Service, and shall comply with clause 8 of the GBG GO Product Terms.

2.2 Data Retention: If Acuant retains any Customer Data at the termination or expiration of the Agreement, at the Customer’s selection, Acuant shall delete or return all Customer Data at the end of the provision of the IDV Services, unless retention is required by applicable law

or for auditing purposes. However, Customer agrees that Acuant may, in its discretion, delete the Customer Data if it determines returning such Customer Data is commercially unreasonable. Acuant retain data for 60 seconds to process the IDV Service. Facematch utilises a sub-processor, Microsoft, who retain data for 24 hours.

2.3 Sub-processors: In providing the IDV Service, Acuant will use the sub-processors outlined in the following table:

Product	Subprocessor	Country (Client may choose location)	Purpose of Processing
AssureID Connect	Amazon Web Services (AWS)	Germany	Cloud Hosting
Face	Amazon Web Services (AWS)	Germany	Cloud Hosting
	Microsoft Azure	Germany	Biometric face matching subprocessor
Liveness	Amazon Web Services (AWS)	Germany	Cloud Hosting

2.4 Biometrics: Face match and Passive Liveness involves processing of biometric data for identity document authentication purposes. This may be a special category of personal data under Applicable Data Protection Law, and therefore may require explicit and affirmative consent to be given by the data subject as a condition for processing such data. It will be the responsibility of the Customer to obtain the data subject’s explicit and affirmative consent on GBG and Acuant’s behalf, inform the data subject of GBG and Acuant’s role, and provide all required transparency disclosures in relation to the processing, which can be found in the Biometric Notice in the following URL: <https://www.idology.com/about-us/product-privacy-policy/>. The Customer will retain records of such data subject’s explicit consent in accordance with Applicable Data Protection Law, which shall not be for a period less than 12 months, and shall provide evidence of consent if requested by GBG or the data subject.

2.5 Details of Processing: the IDV Service shall be provided in accordance with the record of processing table below:

Categories of Personal data Subjects	Customer's end users
Categories of personal data	<p>Contact Information (address)  Location (country)  Personal Identification Information:</p> <ul style="list-style-type: none"> <li>- Name</li> <li>- DOB/age</li> <li>- Gender</li> <li>- Height</li> <li>- Physical Characteristics</li> <li>- Photo</li> <li>- Nationality</li> <li>- National Identification/Registration Number</li> <li>- Driving License Number/Passport Number</li> <li>- Government Issued ID Card information</li> <li>- National Identity Card information</li> </ul> <p>Any data that is included on a medical insurance card or identity document (e.g., passport or driver's license), children included</p>
- Special categories of personal data or sensitive personal data (subject to Applicable Data Protection Law)	- biometric data;
- Frequency of the Transfer	- Personal data will be transferred on a continuous basis in real time when the Customer has a request according to the terms of the Agreement
- Subject Matter of Processing	- The subject matter of processing is as described in the Agreement, in this Product Schedule, and pursuant to Customer's instructions under this Product Schedule.
- Nature of Processing	- The nature of processing is as described in the Customer Use Case , and pursuant to Customer's instructions under this Schedule.
- Purpose(s) of Processing	- The purpose(s) of Processing is as described in the Customer Use Case , and pursuant to Customer's documented instructions.
- Duration	- Within Acuant, data is only retained for 60 seconds. For Facematch, there is a transfer to Microsoft Azure, who retain data for 24 hours.