SCHEDULE 6 - Data Processing Agreement

THIS DATA PROCESSING AGREEEMENT is entered into as of the Effective Date by and between the Parties.

1. INTERPRETATION

1.1. In this Data Processing Agreement, the following terms shall have the meanings set out in this Paragraph 1, unless expressly stated otherwise:`

(a) "**Agreement**" means the Integrator Agreement entered into by and between the Parties that refers to this Data Processing Agreement.

(b) "**Anonymised Data**" means any Client Personal Data, which has been anonymised such that the Data Subject to whom it relates cannot be identified, directly or indirectly, by iProov or any other party reasonably likely to receive or access that anonymised Personal Data.

(c) "**Authorised Sub-processors"** has the meaning given to it in Paragraph 5.1.

(d) "**Biometric Information**" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's Biometric Identifier used to identify an individual.

(e) "**Biometric Information Laws**" means all applicable and binding biometric information laws and regulations as well as government-issued rules, guidelines, directives and requirements currently in effect and as they become effective that may exist in any relevant jurisdiction.

(f) "**Biometric Identifier**" means an individual's physiological, biological, or behavioural characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric Identifiers may include, but are not limited to, imagery of the iris, retina, fingerprint, or face, hand, palm, vein patterns, and voice or video recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(g) "**Cessation Date**" means the end of the Processing or retention period following the date of cessation of any Service involving the Processing of Client Personal Data, as identified in the Retention Schedule.

(h) "**CCPA**" means the California Consumer Privacy Act of 2018 and any binding regulations promulgated thereunder.

(i) "**Controller**" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(j) "**Client Personal Data**" means Personal Data that is Processed by or on behalf of iProov on behalf of Client and governed by the Agreement.

(k) "**Data Protection Legislation**" means the GDPR, and the CCPA.

(l) "**Data Subject Request**" means the exercise by Data Subjects of their rights under, and in accordance with, Chapter III of the GDPR, or the CCPA, in respect of Client Personal Data.

(m) "**Data Subject**" means the identified or identifiable natural person to whom Client Personal Data relates.

(n) "**Delete**" means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed, and "**Deletion**" shall be construed accordingly.

(o) "**EEA**" means the European Economic Area.

(p) "**Effective Date**" means the effective date of the Agreement.

(q) "**GDPR**" means, as and where applicable:

(i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "**EU GDPR**"); and/or

(ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) (the "**UK GDPR**").

References to "**Articles**" and "**Chapters**" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(r) "**Personal Data**" means all information Processed in connection with the Services that constitutes "personal information", "personal data" or any similar term as defined under applicable laws.

(s) "**Personal Data Breach**" means any actual or reasonably suspected breach of security leading to the accidental, unlawful or unauthorized destruction, loss, alteration, encryption, acquisition, disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by the Company in its provision of the Services.

(t) "**Personnel**" means a person's employees, agents, consultants or contractors.

(u) "**Post-cessation Storage Period**" has the meaning given in Paragraph 9.1.

(v) "**Process**" or "**Processing**" means any operation or set of operations which is performed by iProov (or on behalf of iProov) on behalf of Client under this Agreement, on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(w) "**Processor**" means an entity that Processes Personal Data on behalf of a Controller.

(x) "**Retention Schedule**" means the document defining how long Client Personal

Data may be kept in order to provide the Services, as contained in Annex 3.

(y) "**Services**" means those services and activities to be supplied to or carried out by or on behalf of iProov for Client pursuant to the Agreement.

(z) "**Sub-processor**" means any third party appointed by or on behalf of iProov to Process Client Personal Data.

(aa) **"Supervisory Authority"**:

(i) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office;

(ii) in the context of the EEA and EU GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR; and

(iii) any other regulatory, governmental, or independent public authority with jurisdiction over all or any part of (a) the enforcement of Data Protection Legislation; or (b) the Services.

1.2. Unless otherwise defined in this Data Processing Agreement, all capitalised terms in this Data Processing Agreement shall have the meaning given to them in the Agreement (including, for the avoidance of doubt and without limitation, its Schedules).

2. PROCESSING OF CLIENT PERSONAL DATA

2.1. The Parties acknowledge that, as between the Parties, in connection with the Processing of Client Personal Data carried out in the performance of the Services:

(a) iProov acts as a Processor; and

(b) Client acts as the Controller.

2.2. iProov shall:

(a) comply with the Data Protection Legislation in Processing Client Personal Data; and

(b) not Process Client Personal Data other than:

(i) on Client's instructions (subject always to Paragraph 2.88); and

(ii) as required by applicable laws.

2.3. To the extent permitted by applicable Data Protection Legislation, iProov shall inform Client of:

(a) any Processing to be carried out under Paragraph 2.2(b)(ii); and

(b) the relevant legal requirements that require it to carry out such Processing,

before the relevant Processing of that Client Personal Data.

2.4. Client instructs iProov to Process Client Personal Data as necessary:

(a) to provide the Services to Client; and

(b) to perform iProov's obligations and exercise iProov's rights under the Agreement.

2.5.

2.6. **ANNEX 1** (*Data Processing Details*) sets out certain information regarding iProov's Processing of Client Personal Data as required by Article 28(3) of the GDPR.

2.7. Nothing in

2.8. ANNEX 1 (*Data Processing Details*) confers any right or imposes any obligation on any Party to this Data Processing Agreement.

2.9. Where iProov receives an instruction from Client that, in its reasonable opinion, infringes applicable Data Protection Legislation, iProov shall inform Client, unless prohibited from doing so by applicable laws.

2.10. Client acknowledges and agrees that any instructions issued by Client with regards to the Processing of Client Personal Data by or on behalf of iProov pursuant to or in connection with the Agreement:

(a) shall be strictly required to provide the Services or for compliance with applicable Data Protection Legislation; and

(b) shall be consistent with the specifications of the Services to be provided by iProov under the Agreement.

2.11. Notwithstanding anything to the contrary herein, iProov may terminate the Agreement in its entirety upon written notice to Client with immediate effect if iProov considers (in its reasonable discretion) that to adhere to, perform or implement any such instructions would require disproportionate effort (whether in terms of time, cost, available technology, manpower or otherwise).

2.12. Client represents and warrants that it shall provide and maintains all appropriate notices and shall obtain all necessary rights, consents and permissions (including, without limitation, as required by applicable Data Protection Legislation), for Client to make available the Client Personal Data to iProov and for iProov to Process the Client Personal Data as contemplated by the Agreement and this Data Processing Agreement. Client further represents and warrants on an ongoing basis that, with respect to any Processing of Personal Data relating to a Data Subject in the EEA, for the purposes of Article 6 of the GDPR, and (where applicable) Article 9 and/or Article 10 of the GDPR, there shall be a valid legal basis and (where applicable) condition for the Processing by iProov of Client Personal Data in accordance with this Data Processing Agreement and the Agreement.

3. IPROOV PERSONNEL

iProov shall take reasonable steps to require that any iProov Personnel who Process Client Personal Data, are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. SECURITY

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk (which may be of varying likelihood and severity) for the rights and freedoms of natural persons, iProov shall implement appropriate technical and organisational measures in relation to Client Personal Data designed to maintain a level of security appropriate to that risk, including, as appropriate, the measures required by applicable Data Protection Legislation.

4.2. In assessing the appropriate level of security, iProov shall take account in particular of the risks presented by the Processing, in particular from a Personal Data Breach.

4.3. Without limiting the generality of Paragraphs 4.1 and 4.2, iProov shall endeavour to comply with the security measures set out in Annex 2.

5. SUBPROCESSING

5.1. Client generally authorises iProov to use:

(a) the Authorised Sub-processors; and

(b) additional Sub-processors appointed in accordance with this Paragraph 5.

5.2. Client hereby provides a general authorisation to iProov to engage Sub-processors. iProov shall provide Client with a list of such Sub-processors ("**Authorised Sub-processors**") upon demand by Client.

5.3. iProov shall give Client prior notice of any intended addition to or replacement of the Authorised Sub-processors by providing Client with an updated copy of iProov's list of Sub-processors via a 'mailshot' or similar bulk distribution mechanism sent via email to one or more of Client's email addresses referenced in the Agreement. If, within fourteen (14) days of receipt of that notice, Client notifies iProov in writing of any objections (on reasonable grounds) to the proposed appointment, iProov will have twenty-eight (28) days from iProov's receipt of Client's notice to discuss the objection with Client. If, during such twenty-eight (28) day period, Client does not reach an agreement in writing with iProov to permit the use of the relevant Sub-processor or to agree such terms as are proposed by iProov that would apply in order to avoid the use of that Sub-processor, iProov may by written notice to the Client with immediate effect terminate the Agreement either in whole or to the extent that it relates to the Services which require the use of the proposed Sub-processor.

5.4. If Client does not object to iProov's appointment of a Sub-processor during the fourteen (14) day period referred to in Paragraph 5.2, Client shall be deemed to have approved the engagement and ongoing use of that Sub-processor.

5.5. The arrangement between iProov and each Sub-processor is governed by a written contract including terms required by Data Protection Legislation. iProov shall remain liable for any breach of this Data Processing Agreement caused by a Sub-processor.

6. DATA SUBJECT RIGHTS

6.1. Taking into account the nature of the Processing, iProov shall provide Client with such assistance as may be reasonably necessary, technically possible in the circumstances and strictly required under the Data Protection Legislation to assist Client in fulfilling its obligation to respond to Data Subject Requests.

6.2. iProov shall:

(a) promptly notify Client if it receives a Data Subject Request; and

(b) not respond to any Data Subject Request except on the written instructions of Client (and in such circumstances, at Client's cost) or as required by applicable laws.

6.3. Except to the extent prohibited by the Data Protection Legislation, Client shall be fully responsible for any costs arising from iProov's provision of any cooperation and assistance provided under this Paragraph 6, and shall on demand reimburse iProov

any such costs incurred by iProov.

7. PERSONAL DATA BREACHES

7.1. iProov shall notify Client without undue delay (and in any event within seventy-two (72) hours) upon iProov becoming aware of a Personal Data Breach affecting Client Personal Data, providing Client with such information as is required of iProov in its capacity as Processor under applicable Data Protection Legislation (insofar as such information is, at such time, within iProov's possession).

7.2. Upon Client's written request and at Client's expense, iProov will provide Client with co-operation and assistance reasonably requested by Client in connection with any necessary notification of the Personal Data Breach to the relevant Supervisory Authority(ies) and relevant Data Subject(s) (as applicable).

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

8.1. iProov shall provide reasonable assistance to Client with any data protection impact assessments, and prior consultations with Supervisory Authorities, which Client reasonably considers to be required of it by applicable Data Protection Legislation, including Article 35 or Article 36 of the GDPR, in each case solely in relation to the Processing of Client Personal Data by, and taking into account the nature of the Processing by, and information available to, iProov.

8.2. Except to the extent prohibited by Data Protection Legislation, Client shall be fully responsible for any costs arising from iProov's provision of any cooperation and assistance provided under this Paragraph 8, and shall on demand reimburse iProov any such costs incurred by iProov.

9. DELETION OBLIGATIONS AND THE RETENTION SCHEDULE

9.1. Subject to Paragraphs 9.1 and 9.33, upon the Cessation Date, iProov shall immediately cease all Processing of Client Personal Data.

9.2. Subject to Paragraph 9.33, to the extent technically possible in the circumstances (as determined in iProov's sole discretion), iProov shall Delete or irreversibly render Anonymised all Client Personal Data within iProov's possession within thirty (30) days after the Cessation Date.

9.3. iProov and any Sub-processor may retain Client Personal Data where required by applicable law for such period as may be required by such applicable law.

9.4. For the purposes of the Retention Schedule and the Cessation Date that applies to an authentication iProov Product (such as Verifier), an End User qualifies for the authentication iProov Product if:

(a) it executes Enrolment with the Authentication Flag applied; or

(b) it has Passed and executes a Verification through the Verify API during the retention period for the relevant Enrolment.

10. AUDIT RIGHTS

10.1. iProov shall make available to Client within a reasonable period of Client's written request such information as iProov reasonably considers appropriate in the circumstances to demonstrate its compliance with this Data Processing Agreement.

10.2. Subject to Paragraphs 10.3 and 10.4, in the event that Client (acting reasonably) provides documentary evidence that the information made available by iProov pursuant to Paragraph 10.1 is not sufficient in the circumstances to demonstrate iProov's compliance with this Data Processing Agreement, iProov shall allow for and contribute to audits by Client or an auditor mandated by Client in relation to the Processing of Client Personal Data by iProov that are required to assess iProov's performance of this Agreement in accordance with its terms or compliance with Data Protection Legislation (each an "**Audit**"). iProov will provide to internal and external auditors and where relevant Supervisory Authorities (each an "**Auditor**") with such access to Client Personal Data and/or facilities for the Processing of Client Personal Data as are required for conducting an Audit, provided that (a) unless an onsite visit is shown to be necessary, required by applicable law, and consistent with then-current health and safety requirements, any Audit shall be conducted remotely by the provision of access to information by way of screenshots, related information derived from Supplier's books and records relating to compliance with this Agreement, and other online and video-based methods, and (b) any Audit as it relates to an Authorised Sub-processor shall be required to be provided only to the extent permitted by, and subject to the terms of, the related agreement between iProov and the relevant Authorised Sub-processor, and subject to the payment by Client of any related fees or charges that are required to be paid under that agreement.

10.3. Client shall give iProov reasonable notice of any Audit (which shall in no event be less than thirty (30) days' notice unless and to the extent that shorter notice is required by a Supervisory Authority pursuant to Paragraph 10.4(f)) and shall use its best endeavours (and ensure that each of its mandated auditors uses its best endeavours) to avoid causing, and hereby indemnifies iProov in respect of, any damage, injury or disruption to iProov's premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of iProov's other clients or the availability of iProov's services to such other clients) while its Personnel and/or an Auditor's Personnel (if applicable) are on those premises in the course of any on-premise Audit.

10.4. iProov is not required to give access to its premises for the purposes of an audit or inspection:

(a) to any individual unless he or she produces reasonable evidence of their identity and authority;

(b) to any Auditor whom iProov has not given its prior written approval (not to be unreasonably withheld);

(c) unless the Auditor enters into a non-disclosure agreement with iProov on terms acceptable to iProov;

(d) where, and to the extent that, iProov considers, acting reasonably, that to do so would result in interference with the confidentiality or security of the data of iProov's other clients or the availability of iProov's services to such other clients;

(e) outside normal business hours at those premises; or

(f) on more one occasion in any calendar year during the term of the Agreement, except for any additional audits or inspections which Client is required to carry

out under applicable Data Protection Legislation or by a Supervisory Authority.

10.5. Except to the extent prohibited by the Data Protection Legislation, Client shall be fully responsible for any costs arising from iProov's provision of any cooperation and assistance provided under this Paragraph 10 (unless and to the extent that the proximate cause of the relevant Audit is a breach by iProov of this Data Processing Agreement), and shall on demand reimburse iProov any such costs incurred by iProov.

11. PROCESSING PERSONAL DATA OF CALIFORNIA RESIDENTS

11.1. For purposes of this Paragraph 11, the terms "business," "commercial purpose," "sell" and "service provider" shall have the respective meanings given thereto in the CCPA, and "personal information" shall mean Client Personal Data that constitutes personal information governed by the CCPA.

11.2. It is the Parties' intent that with respect to any personal information, iProov is a service provider. iProov shall not (a) sell any personal information; (b) subject to Paragraph 9 retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Service, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Service; or (c) subject to Paragraph 9, retain, use or disclose the personal information outside of the direct business relationship between iProov and Client. iProov hereby certifies that it understands its obligations under this Paragraph 11.2 and will comply with them.

11.3. The Parties acknowledge that iProov's retention, use and disclosure of personal information documented in this Agreement are integral to iProov's provision of the Services and the business relationship between the Parties.

11.4. The Parties acknowledge and agree that iProov's access to personal information is not part of the consideration exchanged by the Parties in respect of the Agreement.

12. BIOMETRIC INFORMATION

12.1. Client shall ensure that, prior to or at the point of collection, all relevant Data Subjects for whom Biometric Information may be Processed are adequately notified, as required by applicable Biometric Information Laws and Data Protection Legislation, that Biometric Information may be collected from them, and of iProov's Processing of Biometric Information.

12.2. Client shall ensure that it has a valid legal basis and obtained all necessary rights, consents and permissions for the Processing of Biometric Information, including iProov's Processing of Biometric Information, prior to or at the point of collection of Biometric Information, as required by the Data Protection Legislation and all applicable Biometric Information Laws.

12.3. Client warrants and represents that any instructions issued by Client with regards to the Processing of Biometric Information by or on behalf of iProov pursuant to or in connection with the Agreement shall comply with applicable Biometric Information Laws and Data Protection Legislation.

13. INCORPORATION AND PRECEDENCE

13.1. This Data Processing Agreement shall be incorporated into and form part of the Agreement with effect from the Effective Date.

13.2. In the event of any conflict or inconsistency between this Data Processing Agreement and the remainder of the Agreement, the provisions in this Data Processing Agreement shall prevail to the extent of such conflict or inconsistency.

14. CHANGE IN CONDITIONS

If iProov:

(a) determines that it is unable for any reason to comply with its obligations under this Data Processing Agreement and iProov cannot cure this inability to comply using commercially reasonable efforts; or

(b) becomes aware of any circumstance or change in law that is likely to have a substantial adverse effect on iProov's ability to meet its obligations under this Data Processing Agreement,

iProov may notify Client thereof, in which case iProov will have the right to temporarily suspend its and/or any Sub-processor's Processing of Client Personal Data, without liability, until such time that such Processing is adjusted in such a manner that the non-compliance is remediated. To the extent such adjustment is not performed within twenty-eight [28] days of iProov's notification to Client, either Party shall have the right to terminate the relevant part of such Processing by iProov and/or any Sub-processor.

15. LIABILITY

The total aggregate liability of either Party towards the other Party, howsoever arising, under or in connection with this Data Processing Agreement will under no circumstances exceed any limitations or caps on, and shall be subject to any exclusions of, liability and loss agreed by the Parties in, the Agreement.

ANNEX 1

DATA PROCESSING DETAILS

This Annex 1 includes certain details of the Processing of Client Personal Data as required by Article 28(3) GDPR.

iProov Details

Name:	As set out in the pre-amble to the Agreement
Address:	As set out in the pre-amble to the Agreement
Contact Details:	compliance@iproov.com
iProov Activities:	iProov is a provider of a technology solution that is utilised to deliver genuine presence and/or liveness assurance services to Client.
Role (controller/processor):	Processor – in relation to Processing of Client Personal Data on behalf of the Client.

Client Details

Name:	As set out in the pre-amble to the Agreement
Address:	As set out in the pre-amble to the Agreement
Contact Details:	As set out under the Agreement
Client Activities:	As set out under the Agreement
Role (controller/processor):	Controller

Details of Processing

Categories of Data Subjects:	The End Users of the Client and any Third Party Client
Categories of Personal Data:	• Personal details, including any information that identifies the data subject and their personal characteristics. • Markers as to estimated ethnicity, race, age and/or sex. • Personal details issued as an identifier by a public authority, including passport details,

	national insurance numbers, identity card numbers, driving licence details. • IP address of the Data Subject's device connected to the iProov Product. • Facial imagery of the Data Subject created when using the Enroller or the Verifier iProov Products • Pseudonymous user name of the Data Subject. • An identifier of an installed instance of an Android, IOS or HTML5 SDK. • Biometric template.
Sensitive Categories of Data:	Biometric Information used to identify Data Subjects
Nature of the Processing:	• Receiving data, including collection, accessing, retrieval, recording, and data entry • Holding data, including storage, organisation and structuring • Using data, including analysing, consultation, testing, automated decision making and profiling • Erasing data, including destruction and deletion
Purpose of the Processing:	Performing the Services, as described in the Agreement.
Duration of Processing / Retention Period:	As long as needed to perform the Services under the Agreement and in accordance with the Retention Schedule.

ANNEX 2

SECURITY MEASURES

iProov will implement and maintain ISO/IEC 27001:2013 the scope of which will include the iProov Technologies provided to the Client including the following standards:

1. ISO/IEC 27001:2013 section 5.3 - Organizational roles, responsibilities and authorities
2. ISO/IEC 27001:2013 section 8.2 – Information security risk assessment
3. ISO/IEC 27002:2013 section 9 – Access control
4. ISO/IEC 27002:2013 section 10 – Cryptography
5. ISO/IEC 27002:2013 section 9.2.4 - Management of secret authentication information of users
6. ISO/IEC 27002:2013 section 11.1 – Management of secure areas
7. ISO/IEC 27002:2013 section 12.1.2 - Change management
8. ISO/IEC 27002:2013 section 16.1 - Management of information security incidents and improvements
9. ISO/IEC 27002:2013 section 13.1 - Network security management
10. ISO/IEC 27002:2013 section 12.6 – Technical vulnerability management
11. ISO/IEC 27002:2013 section 17 - Information security aspects of business continuity management.

iProov may update or modify these security measures from time to time provided that such updates and modifications do not materially decrease the overall security of the services and/or relevant Client Personal Data.

ANNEX 3

RETENTION SCHEDULE

Description	Retention Time	Purposes	ML Training**	Authorised Research Methodology*
Facial Imagery	30 Days except auth***	Providing the Services including the results of authentication attempts	N	
		Investigate and Identify potential and actual attacks against Services retrospectively, allowing iProov to make Client aware of sustained attacks and if applicable provide transaction details for successful attacks	N	
		Test performance of new security tests before making part of automated decision process	N	
		Use for creation of new/updated security tests where required to protect end users against systemic attacks on Services	Y	Optimising performance according to ISO/IEC 30107-3:2017 or successor
		Use for optimisation of new/updated security tests to minimise bias	Y	Optimising performance according to ISO/IEC 30107-3:2017 or successor
		To measure any bias within Services to allow iProov to demonstrate its lack of material bias	N	
		To improve system performance of Services in real time response by minimising bias	N	
		Use for creation of new/updated security tests where required to minimise bias	Y	Optimising performance according to ISO/IEC 30107-3:2017 or successor
Biometric Profile	30 Days except auth***	Providing Services and the results of authentication attempts	N	
		Investigate and Identify potential and actual attacks against the Services	N	
		To test updated face matchers before live implementation to prove performance for end users of Services	N	
Markers s to estimated ethnicity, ace, age and/or sex	30 Days except auth***	To measure any bias within Services to allow iProov to demonstrate its lack of material bias	N	
		To improve system performance of Services in real time response by minimising bias	N	
		Use for creation of new/updated security tests where required to minimise bias	Y	Optimising performance according to ISO/IEC 30107-3:2017 or successor
Pseudonymised username provided by Controller	30 Days except auth***	To link Facial Imagery with Biometric Profile	N	
The IP address of a device connecting to the Services	12 months except auth***	To allow troubleshooting and support	N	
An identifier of an installed instance of an Android, iOS or HTML5 SDK	12 months except auth***	To allow troubleshooting and support	N	

*Client authorises iProov to deploy these Authorised Research Methodologies for the training of Services to help eliminate bias and protect against fraudulent attacks on Services
** Whether the data is used for Machine Learning training/testing to improve system performance.
***For iProov Authentication the data is retained and processed until (a) termination of the Agreement, or (if earlier) (b) deletion of the relevant End User