Date:

International Tennis Integrity Agency Ltd

as ITIA

[……]

as Company

Data Sharing Agreement

THIS AGREEMENT is made the [……] day of [……] 20[…..]

BETWEEN:

(1) **INTERNATIONAL TENNIS INTEGRITY AGENCY LTD**, a company incorporated and registered in England and Wales with company number 13057428 whose registered office is at Fieldfisher Riverbank House, 2 Swan Lane, London, United Kingdom, EC4R 3TT (as "**ITIA**"); and

(2) [Company Name and registration number]

[address of registered office]

The above company with its registered office at the address above shall hereinafter be referred to as "**Company**";

each a "**Party**" and together the "**Parties**" (the "Agreement").

BACKGROUND:

(A) The ITIA is the independent professional tennis integrity organisation established to promote and protect the integrity of international professional tennis with, *inter alia,* responsibility for investigating and prosecuting under the TACP (as defined below).

(B) The Company is a betting company under an obligation to report unusual or suspicious betting activity to ITIA arising from its relationship with any Covered Events Governing Body and/or data company authorised by any such Covered Events Governing Body.

(C) As a result of such obligation, the Parties are transferring Data between themselves for the Permitted Purpose(s).

(D) The Parties acknowledge that, for the purposes of this Agreement, they are each independent Controllers with respect to Data Processed for the Permitted Purpose(s).

(E) The purpose of this Agreement is to set out the data protection terms that will apply to any such transfer, in order to ensure that the data protection rights and freedoms of individuals remain protected in accordance with Data Protection Laws. This Agreement also sets out the integrity protection measures that are relevant to the Company.

IT IS AGREED:

1. Definitions

In this Agreement:

"**Controller**" means an entity that alone or jointly with others determines the purposes and means of Processing of Personal Data.

"Covered Events Governing Body" means a Governing Body and/or a Covered Event Organizer (and/or its affiliate).

“Covered Event” means those professional tennis matches and other tennis competitions listed in Appendix 1 of the TACP

“Covered Event Organizer” means any party other than the Governing Bodies which has been approved as a Covered Events organizer by the ITIA Board in relation to event(s) listed in Appendix 1 of the TACP.

"**Data Protection Laws**" means all laws applicable (in whole or in part) to a Party's Processing of Personal Data under or in connection with this Agreement, including, as applicable EU Data Protection Law and UK Data Protection Law, as introduced, amended or superseded from time to time.

"**Data**" means any Trend Data, and/or any Personal Data for which the ITIA or the Company are Controllers shared under this Agreement as described and defined in Schedule 1 (Permitted Purpose).

"**Effective Date**" has the meaning given at the top of this Agreement.

"**EU Data Protection Law**" means (i) all EU regulations or other legislation applicable (in whole or in part) to the Processing of Personal Data (such as Regulation (EU) 2016/679 (the "**EU GDPR**")), (ii) the national laws of each EEA member state implementing any EU directive applicable (in whole or in part) to the Processing of Personal Data (such as Directive 2002/58/EC (the "**e-Privacy Directive**")), and (iii) any other national laws of each EEA member state applicable (in whole or in part) to the Processing of Personal Data, in each case as amended or superseded from time to time.

“Governing Body” means a tennis governing body in membership of the ITIA in accordance with the ITIA’s articles.

"**Permitted Purpose(s)**" means the ITIA Permitted Purpose and the Company Permitted Purpose.

"**Personal Data**" means any information relating to an identified or identifiable natural person and includes the categories of data listed in Schedule 1 (Permitted Purpose(s)). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Process**", "**Processing**" or "**Processed**" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means an entity that Processes Personal Data on behalf of, and in accordance with, the instructions of a Controller.

"**Restricted Transfer**" means (i) where the EU GDPR applies, a transfer of Personal Data to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

"**Standard Contractual Clauses**" means

(a) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj (the "**EU SCCs**"); and

(b) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the DPA 2018 (the "**UK Addendum**").

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Data.

"**Security Measures**" means the security measures specified in Schedule 2 (Security Measures) as may be updated or reissued from time to time.

"**Supervisory Authority**" means the relevant data protection supervisory authority with responsibility for enforcing Data Protection Laws in the territory of the ITIA and/or the Company, as applicable.

"**TACP**" means the Tennis Anti-Corruption Program (as may be amended, superseded or replaced from time to time) and as published at www.itia.tennis.

"Tennis Data" means live match scores and related statistical data from any Covered Event generated by or on behalf of a Covered Events Governing Body.

"Trend Data" means any anonymous data relating to trends in and/or threats to the integrity of professional tennis or specific tournaments or tours of professional tennis.

"**UK Data Protection Law**" means (i) the GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**"), (ii) the Data Protection Act 2018 (the "**DPA 2018**"), (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 as they continue to have effect by virtue of section 2 of the European Union (Withdrawal) Act 2018 ("**PECR**"), and (iv) any other laws in force in the UK from time to time applicable (in whole or in part) to the Processing of Personal Data, in each case as amended or superseded from time to time.

2. Relationship of the Parties

2.1 The Parties are each considered independent Controllers of the Data that is being Processed for the Permitted Purpose(s) under this Agreement.

2.2 In relation to Processing of the Data for the Permitted Purposes they have determined their respective responsibilities to data subjects as set out in Schedule 1.

3. Permitted Purposes

3.1 The Parties acknowledge and agree that:

(a) the ITIA shall be permitted to use the Data shared pursuant to this Agreement in connection with its disciplinary and/or integrity related investigations and prosecutions, the maintenance of the no credentials list and related activities concerning integrity in tennis (together, "**ITIA Permitted Purposes**") and may share this information for such purposes with (and only with) the persons set out in Part C (ITIA) of **Schedule 1**; and

(b) the Company shall be permitted to use the Data shared pursuant to this Agreement (including any Personal Data) to investigate and fulfil any requests made by the ITIA and in connection with its own investigations and prosecutions ("**Company Permitted Purposes**") and may share this information for such purposes with (and only with) the persons set out in Part C (Company) of **Schedule 1**.

4. Company Obligations

4.1 Subject to clause 4.2, the Company shall:

(a) promptly report to the ITIA any unusual or suspicious betting activity it is or becomes aware of in connection with any Covered Event;

(b) promptly make available to the ITIA any betting related information (including any Data and/or Tennis Data) in connection with any Covered Event that the ITIA reasonably requests for intelligence purposes and for use in disciplinary proceedings;

(c) promptly report to the ITIA by providing it with any Data controlled by the Company in connection with any Covered Event where:

(i) the data subject(s) of that Data matches any Covered Person (as defined in the TACP) or ITIA person of interest which has been provided to the Company by the ITIA following a reasonable request by the ITIA; and/or

(ii) the Company itself becomes aware that a Covered Person has participated in tennis betting;

(d) [in relation to any Tennis Data which has been purchased by the Company from a Covered Events Governing Body and/or data company authorised by a Covered Events Governing Body,] develop and maintain its own risk management lists and policies for the removal of (at least) in-play betting on players or Covered Event matches of concern at its discretion in accordance with its own policy;

(e) in relation to any Tennis Data which has been purchased by the Company from a Covered Events Governing Body and/or data company authorised by a Covered Events Governing Body for a purpose related to facilitating tennis betting:

(i) not make, or facilitate the making of, betting markets for Covered Events Governing Bodies' tennis events for which Tennis Data are not being sold (for example, without limitation, under 18 junior events); and

(ii) not make, or facilitate the making of, betting markets for any Covered Event that the ITIA and the relevant Covered Events Governing Body, in consultation, reasonably direct should not be made, having consulted with the relevant data company and/or (where applicable) betting regulator and/or law enforcement agency; and

(f) take all reasonable steps with the relevant data company, Covered Events Governing Body and the ITIA to safeguard the integrity of the sport of tennis.

In each case, any exchange of information shall be strictly in accordance with the terms of this Agreement.

4.2 The Company is not obliged to provide any Personal Data to ITIA where there is a legally binding request from a public authority not to disclose. Where this does apply, the Company shall, to the

extent legally permitted, notify ITIA of the fact and use reasonable endeavours to waive the prohibition.

5. Responsibilities of the Parties

5.1 Each Party shall provide reasonable assistance to the other as may be required in order to enable each Party to perform its responsibilities pursuant to this Agreement.

5.2 When Processing Data under this Agreement, each Party warrants that:

(a) it has all necessary rights, permissions and/or licenses to Process the Data as a Controller for their respective Permitted Purposes;

(b) it will comply with any requirements arising Data Protection Laws to protect the Data it Processes under this Agreement; and

(c) it will comply with its obligations as set out in Schedule 2 (Security Measures) to this Agreement.

5.3 Each Party shall Process the Data respectively only for their respective Permitted Purposes or as otherwise permitted under Data Protection Laws.

5.4 If a Party wishes to Process the Data for a new or different purpose other than the Permitted Purposes (an "**Alternative Purpose**"), it may do so provided it first informs the other Party about its intention to Process Data for an Alternative Purpose and does all such acts and things as are necessary to ensure that its intended Processing of the Data for the Alternative Purpose fulfils the requirements of Data Protection Laws (including by obtaining any consents from Data Subjects, where necessary). Provided such requirements are met, the Alternative Purpose shall be deemed a Permitted Purpose.

5.5 Each Party shall cooperate with the competent Supervisory Authority if and as needed.

5.6 Neither Party shall knowingly perform its obligations under this Agreement in such a way as to cause the other Party to breach any of its obligations under Data Protection Laws.

6. Appointment of Processors

6.1 Each Party (the "**Appointing Party**") may appoint one or more third party Processors to process the Data on its behalf, provided that:

(a) the Processor provides sufficient guarantees that it will implement appropriate technical and organisational measures to Process the Data in compliance with Data Protection Laws;

(b) the Processor enters a written contract with the Appointing Party that: (i) requires the Processor to process the Data only on instructions from the Appointing Party; (ii) requires the Processor to implement appropriate technical and organisational measures to protect the Data against a Security Incident; and (iii) conforms with Data Protection Laws in all other respects;

(c) the Appointing Party accepts liability for all Processing of the Data conducted by its Processor(s) and for any breach of this Agreement that is caused by an act or omission of its Processor(s); and

(d) the Appointing Party maintains a list of all Processors it appoints, including the Processing activities they fulfil, and provides such list to the other Party upon request.

7. Restricted Transfers of Data

7.1 The Parties agree that where a party makes a Restricted Transfer to the other Party, that Restricted Transfer shall be subject to the appropriate Standard Contractual Clauses as set out in either clause 7.2or clause 7.3below.

7.2 Where a Restricted Transfer is subject to the EU GDPR, the EU SCCs will be deemed entered into between the Party transferring the Personal Data (as "data exporter") and the Party receiving the Personal Data (as "data importer") and completed as follows:

(a) Module One will apply;

(b) in Clause 7, the optional docking Clause will not apply;

(c) in Clause 11, the optional language will not apply;

(d) in Annex I:

(i) Part A: with the information set out in Part A of Schedule 1 to this Agreement;

(ii) Part B: with the information set out in Part B of Schedule 1 to this Agreement; and

(iii) Part C: in accordance with the criteria set out in Clause 13(a) of the Standard Contractual Clauses; and

(e) Annex II: with the information set out in Schedule 2 to this Agreement.

7.3 Where the Restricted Transfer is subject to the UK GDPR: the UK Addendum will be deemed entered into between the Party transferring the Personal Data (as "data exporter") and the Party receiving the Personal Data (as "data importer") and completed as follows:

(a) the EU SCCs, completed as set out above in clause 7.2, shall also apply to transfers of such Personal Data, subject to sub-clause (b) below;

(b) Tables 1 to 3 of the UK Addendum shall be deemed completed with the relevant information from the EU SCCs, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the Effective Date.

7.4 If there is any conflict between this Agreement and the Standard Contractual Clauses applicable to any Party's transfer of Personal Data to the other Party, those Standard Contractual Clauses will prevail.

8. Termination

This Agreement will remain in place for as long as the Company has an agreement in place with a Covered Events Governing Body and/or a data company authorised by a Covered Events Governing Body in relation to the receipt of Tennis Data. Termination of this Agreement (however caused) shall not affect the continuing in force of obligations relating to Data shared prior to the date of termination.

9. Indemnification

Each Party will indemnify and keep indemnified the other in respect of all and any claims, proceedings or actions brought against it arising out of any breach by the other Party of its obligations relating to data protection under this Agreement.

10. Confidentiality

10.1 For the purposes of this Clause 10.1, "Confidential Information" shall mean in relation to each Party, all information (whether written, oral or obtained by observation or another means and whether directly or indirectly) whether disclosed/obtained before, on, or after the date of this Agreement which concerns the business, financial affairs, operations, suppliers or customers of that Party or which is otherwise confidential in nature, including the existence and provisions of this Agreement.

10.2 Each Party undertakes (both during and after the Term) to keep confidential any Confidential Information relating to the other Party which it obtains under or in connection with this Agreement and not to use such information or disclose it to any other person, other than as permitted under this Clause 10.

10.3 Each Party may disclose Confidential Information relating to the other Party:

(a) to its employees, sub-contractors, officers, representatives or advisors who need to know such information for the purpose of exercising that Party's rights or carrying out its obligations under or in connection with this Agreement. Each Party shall ensure that its employees, sub-contractors, officers, representatives and/or advisors to whom it discloses the other Party's Confidential Information comply with this Clause 10;

(b) if such Confidential Information has come into the public domain other than by a breach of any obligation of confidentiality;

(c) as may be required by law, a court or any governmental or regulatory authority (in each case subject to the same being of competent jurisdiction); or

(d) with the prior written approval of the other party.

10.4 The restrictions contained in this Clause shall continue to apply after the termination or expiry of this Agreement (however arising) without limit in time.

11. Notices

11.1 Any notice or other communication given to a Party under or in connection with this Agreement shall be in writing, addressed to the individual(s) identified at Clause 11.2 below and shall be:

(a) delivered by hand or by pre-paid registered first-class post to the other Party's registered office; or

(b) sent by email (save that any notice alleging a dispute or purporting to terminate or vary this Agreement will only be valid if accompanied by the same notice given by a delivery method set out in (a) above).

11.2 For the purposes of Clause 11.1, all notices served under this Agreement shall be sent to the following individual (or such other individual as notified in writing by the relevant Party from time to time):

(a) ITIA – Ben Rutherford ben.rutherford@itia.tennis or Kirsty Batchelor, kirsty.batchelor@itia.tennis or dpo@itia.tennis

(b) Company – [NAME AND EMAIL ADDRESS]

11.3 Any notice or communication shall be deemed to have been received (i) if delivered by hand, on signature of a delivery receipt; (ii) if sent by pre-paid registered first-class post, on the date of successful delivery, as evidenced by a delivery receipt; and (iii) if sent by email, at 9.00 am on the next working day after transmission.

12. Miscellaneous

12.1 Clause headings and other headings in this Agreement are for convenience of reference only and will not constitute a part of or otherwise affect the meaning or interpretation of this Agreement.

12.2 Schedules to this Agreement will be deemed to be an integral part of this Agreement to the same extent as if they had been set out in full within this Agreement.

12.3 This Agreement and the attached Schedules executed by the Parties, constitute the entire agreement between the Parties relating to the subject matter of this Agreement and supersede all prior agreements, understandings, negotiations and discussions of the Parties.

12.4 The provisions of this Agreement are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability will affect only such phrase, clause or provision, and the rest of this Agreement will remain in full force and effect.

12.5 The provisions of this Agreement will endure to the benefit of and will be binding upon the Parties and their respective successors and assigns.

12.6 This Agreement may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

12.7 In the event of a conflict or inconsistency between the terms of this Agreement and any terms of another agreement covering the Company's obligations to report unusual or suspicious betting activity to ITIA, this Agreement shall prevail.

12.8 This Agreement will be governed by and construed in accordance with the laws of England and Wales. The Parties agree to irrevocably submit any dispute arising in connection with this Agreement (including any dispute or claim relating to non-contractual obligations) to Sport Resolutions UK for arbitration pursuant to the Full Arbitration Procedure in accordance with the Sport Resolutions Arbitration Rules then in force, provided that there shall be only one (1) arbitrator, the proceedings shall be conducted in English, and the location for the arbitration shall be London, England.

12.9 This Agreement has been signed on behalf of each of the Parties by a duly authorised signatory.

SIGNED for and on behalf of **ITIA**:

.....

Signature

.....

Print name

.....

[Title]

SIGNED for and on behalf of **Company**:

.....

Signature

.....

Print name

.....

[Title]

Schedule 1

Permitted Purpose(s)

This Schedule 1 describes the types of Personal Data Processed under this Agreement. This Schedule is subject to the terms of this Agreement entered into by the Parties. Capitalised terms not defined in this Schedule will have the meaning attributed to them in the Agreement.

LIST OF PARTIES

1.	Name:	ITIA
	Address:	As per the Agreement.
	Contact person's name, position and contact details:	Ben Rutherford, Senior Director, Legal ben.rutherford@itia.tennis Kirsty Batchelor, Head of Business Services kirsty.batchelor@itia.tennis dpo@itia.tennis
	Activities relevant to the data transferred under these Clauses:	As per the Permitted Purposes set out in clause 3 of this Agreement.
	Signature and date:	See signature block to this Agreement.
	Role (controller/processor):	Controller

1.	Name:	[To be completed]
	Address:	As per the Agreement
	Contact person's name, position and contact details:	[To be completed]
	Activities relevant to the data transferred under these Clauses:	As per the Permitted Purposes set out in clause 3 of this Agreement.
	Signature and date:	See signature block to this Agreement.

	Role (controller/processor):	Controller

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	Tennis players; related person including coach, trainer, therapist, physician, management representative, agent, family member, tournament guest, business associate or other affiliate or associate of any player, any other person who receives accreditation at a TACP Covered Event at the request of the player or any other related person; tournament support personnel; and attendees at Covered Events. ITIA's employees and contractors. [Company's customers, employees and contractors.]
Categories of personal data transferred:	Full name, contact details (email address and telephone number), player IDs, account information and statements, images, video, match results, injury data, match statistics, training details, equipment used. [Company to add any other personal data categories which it may share with the ITIA].
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	The Personal Data Processed concern the following categories of special category data: (a) ITIA – some or all of special category data or personal data relating to criminal convictions and offences (e.g. bribery or corruption convictions) and/or health data (e.g. gambling addiction, injury information or medical examinations) may be processed; and (b) Company – some or all of special category data or personal data relating to criminal convictions and offences (e.g. bribery or corruption convictions) and/or health data (e.g. gambling addiction, injury information or medical examinations) may be processed. Please see security measures and purpose limitation clauses for safeguards.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous.
Nature of the processing:	[To be completed]
Purpose(s) of the data transfer and further processing:	The Personal Data is Processed for the Permitted Purposes set out in clause 3 of this Agreement.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Personal Data will be retained in accordance with the Party's respective data retention policy and in any event, no longer than is required for the permitted purposes.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Not applicable.

C. PERMITTED RECIPIENTS

ITIA

ITIA is permitted to disclose the information shared by Company pursuant to this Agreement with the following persons or category of persons:

a) Betting operators and regulators;

b) Law Enforcement Agencies and Regulators in connection with the prevention or detection of crime or the apprehension or prosecution of offenders;

c) Covered Events Governing Bodies and/or their lawyers;

d) United Kingdom's Gambling Commission and other betting regulators;

e) Grand Slam Board;

f) Professional Tennis Integrity Officers;

g) Covered Persons (and their legal advisors);

h) Data Supply Companies who provide data to betting operators under contract with a Covered Events Governing Body(ies);

i) International Olympic Committee (where the data relates to an Olympic event), International Paralympic Committee (where the data relates to a Paralympic event) and other major event organisers recognised by a Governing Body; and

j) ITIA's service providers and suppliers who provide services to it or on its behalf (e.g. legal advisors and the ITIA's European Representative; translation and transcriber service providers, forensic service providers, IT providers, website and app hosting company and similar; and other bodies in connection with specific data sharing activities, consistent with the role of the ITIA from time to time.

Company

Company is permitted to disclose the information shared by ITIA pursuant to this Agreement with the following persons or category of persons:

a) [•]; and

b) in other circumstances, where the Company has obtained the prior written consent of the ITIA.

Schedule 2

Security Measures

This Schedule describes the security measures that the Parties will comply with when Processing Data as set out under this Agreement. This Schedule is subject to the terms of this Agreement.

1. Security Governance

1.1 A Party will be responsible for the selection, implementation and maintenance of security procedures and policies that are sufficient to ensure that connection to the other Party's network is secure and is used only for authorised purposes, and that the other Party's records and data are protected against improper access, use, loss, alteration or destruction.

1.2 A Party will not transmit information that that Party knows or suspects to be unacceptable within the context and purpose for which it is being communicated, and unless required to by law, not process any Data for any purpose other than those set out under this Agreement.

1.3 Processes and Technologies will be implemented with Security and Privacy by design.

1.4 Each Party's staff will be appropriately educated to understand principles of Privacy and Security.

2. Physical security

2.1 In place 24 x7 (e.g. premises, server room access controls, alarms, power supply etc.)

2.2 Card access systems; restricted access to employees and cleared contract personnel

2.3 Server rooms are controlled by door access systems, limited to approved personnel only.

2.4 Data Centre server rooms are fitted with appropriate environmental controls; Universal Power Supply (UPS) as standard.

2.5 Controlled fire / emergency alarm systems throughout offices

2.6 CCTV in place and recorded for strategic areas.

3. Internal network security (e.g. network traffic limitation, data storage, anti-malware, data segmentation)

3.1 Default credentials are changed prior to deployment and remote connection to devices is via secured method.

3.2 Network is run over private data connections.

3.3 Ingress / egress points are controlled by next generation firewalls, Intrusion Prevention Systems (IPS/IDS) and are monitored 24/7

3.4 Data storage devices are protected via advanced anti-virus software; access is controlled via directory services.

4. Server and application security (e.g. password protection encryption, protection against admin error as well as external attack, backup and supported by policies)

4.1 Servers and applications are deployed with latest OS, firmware, software within the respective Party's supported versions.

4.2 Data storage devices are protected via advanced anti-virus software; access is controlled.

4.3 Data is backed-up on a regular cycle with backups held in a remote location.

4.4 External attacks mitigated by a number of methods including Next Generation firewalls, web application firewalls, IPS and 24/7 monitoring.

4.5 Encryption is in place in transit and at rest where practicable: minimum levels to be agreed and each Party to advise and who will hold the encryption keys (reside in the EU/EEA)

5. Access controls (e.g. authorisation profiles, withdrawing access when someone leaves)

5.1 A team manages user account creation / removal, change and data access controls.

5.2 Access is based on the principle of least privilege and users shall only access data to fulfil role.

5.3 Access is granted to individuals and accounts and passwords are handled and protected as confidential data.

5.4 Multi-Factor authentication

6. Workstation security (e.g. firewall software, automatic session locking, device hardening)

6.1 User devices are covered by virus and malware protection including defence against advanced persistent threats.

6.2 Automatic session locking is in place.

6.3 All user devices are built from image templates with latest updates for software and OS.

6.4 Firewall software is implemented on all user devices.

6.5 All mobile devices are encrypted.

7. Data access monitoring (e.g. abnormality detection, remote access, DLP)

7.1 Remote access is controlled through a number of prescribed methods such as: Secure VPN tools, Remote portal technologies, Supervised remote sessions.

7.2 Abnormal behaviour detection

7.3 Access logging / monitoring in place e.g. SOC / SIEM

7.4 Privileged access management reviews

8. Resilience and continuity planning

8.1 Remote back-ups and data replication

8.2 Back-up policy and processes

8.3 Minimised single points of failure and services secure with redundancy built into design.

8.4 Disaster recovery plans in place and tested regularly.

8.5 Maintenance and servicing measures are in place for all services and systems.

9. Mobile processing (e.g. VPN access, disk/file encryption, removal from mobile devices)

9.1 All mobile devices have disk level encryption.

9.2 Mobile computer devices have VPN access via a dedicated VPN client.

9.3 Mobile devices are registered on policy controlled via mobile device management systems.

10. Personnel Security

10.1 Mandatory Information Security and Data Protection training for those in roles handling sensitive or personal information or for individuals with privileged access – e.g. HR, Finance, IT etc.

10.2 Appropriate technical training for staff to fulfil their roles.

11. Asset disposal

11.1 Hardware assets are disposed of responsibly, securely and verifiably through accredited third party partners.

11.2 Software assets are retired and removed from service securely.

12. Incident response

12.1 Defined data breach and incident policies. Response processes with designated incident response owners and managers throughout the business.

12.2 Response processes tested regularly.

12.3 Under UK GDPR, organisations should notify the ICO "without undue delay and in any event no later than 72 hours after [becoming] … aware that an incident has occurred".

13. Standards (e.g. ISO27001)

Developed security infrastructure using industry standards and guidelines such as:

(a) ISO27001, NIST, Cyber Essentials+

(b) Penetration and vulnerability assessments by CREST approved companies (or similar local equivalent).

(c) Supplier will provide current certificates on request and upon any changes to status.

14. Laws and regulation

Each Party will comply with local laws and regulations.