Black Box Data Imaging Solutions LLP

CLIENT DATA PROCESSING AGREEMENT

in accordance with the relevant contractual terms for processors and controllers required by the General Data Protection Regulation ("GDPR")

AGREEMENT SUMMARY	
Agreement Number	
Controller (The Client)	????
Processor	Black Box Data Imaging Solutions LLP. (Processor) – Partnership No. OC349857
Start Date	????
Estimated End Date	????
Term	This Agreement shall commence on the Start Date and shall continue for the duration of the agreement
Subject-matter	Scanning of ?????
Type of the personal data	????
Nature and purpose of the processing	Scanning of paper files (digitisation)
Categories of data subjects	See schedule III.
Retention period	No data/documents are to be retained by the Processor. Upon scanned files being successfully transferred to the Client all the Client data will be permanently deleted from the Processors equipment.
Appropriate technical and organisational measures taken by processor	???? See Appendix
Approved Sub processors	
Survival clauses	**Clause 1: DEFINITION** **Clause 2 (1): PROCESSOR** **Clause 5: RIGHTS OF DATA SUBJECTS** **Clause 7: LIABILITY AND INDEMNITY** **Clause 10: ENFORCEABILITY** **Clause 14: LAW AND JURISDICTION**
Jurisdiction	**England**
The Client Contact Details	
Processor Contact Details	Data Processing Officer – Black Box Data Imaging Solutions LLP.
Processor Address	Pole Barn Office, Parsonage Farm, Boughton Monchelsea, Kent, ME17 4JB
Project Manager (PM)	?????

GENERAL TERMS PROCESSING AGREEMENT

A. The Client in order to execute its business, uses/stores personal data.
B. The Processor is a specialist services company in document imaging.
C. Parties have agreed under the Main Agreement that processor shall the process data for the Client as mentioned in the Agreement Summary.
D. This Agreement is subject to the GDPR, more specific the relevant contractual terms required of processors and controllers (Articles 28, 32 and 33 of the GDPR) and all applicable national and/or local legislation regarding data protection.
E. This Agreement sets out the terms and conditions that specify or apply in addition to the GDPR and the national and local data protection legislation.
F. All agreements made by Parties regarding the processing of personal data are governed by this Agreement.
G. This Agreement is concluded within the context of the Main Agreement processor entered with the Client or any of its subsidiaries. If there are any conflicts between the provisions of this Agreement and the provisions of the Main Agreement the provisions of this Agreement will take precedence.

1. DEFINITIONS

1.1. Lower case terms used but not defined in this Agreement, such as "personal data", "personal data breach", "processing", "controller", "processor", and "data subject", will have the same meaning as set forth in Article 4 GDPR.
1.2. For the purpose of this Agreement the terms used in the Agreement Summary will have the meaning as set forth in the Agreement Summary:
1.3. For the purpose of this Agreement:
"Affiliate" means in relation to a party, its parent undertaking or its subsidiary undertaking or a subsidiary undertaking of its parent undertaking, in each case from time to time ("subsidiary undertaking" and "parent undertaking" have the meanings set out in sections 1161 and 1162 of and Schedule 7 of the Companies Act 2006 or as defined in the equivalent legislation in the Jurisdiction detailed in the Agreement Summary).
"Agreement" means the Agreement Summary, these terms, and all Schedules to this agreement.
"Agreement Summary" means the section entitled 'Agreement Summary' at the beginning of this Agreement.
"Main Agreement" means the service contract including amongst others the processing of personal data as described in the Agreement Summary.
"Parties" mean The Client and Processor.
"Schedule" means the schedules to this Agreement.
"Sub processor" means the other processors that are used by processor to process personal data.

2. PURPOSE(S) FOR PROCESSING PERSONAL DATA

2.1 Parties have determined the purpose(s) for the processing of personal data under both this Agreement and the Main Agreement in **Schedule III** of this Agreement. Processor shall in line with Article 28 (3) GDPR process the personal data only on documented instructions from the Client and for no other purpose than the purpose(s) defined in **Schedule III** and in accordance with the GDPR and all applicable national and/or local laws, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by the European Union or other applicable national and/or local legislation to which processor is subject; in such a case, processor shall inform the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

3. PROCESSOR

3.1 In line with the other requirements of Article 28 (3) GDPR, processor shall:
(a) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
(b) not disclose the personal data to third parties without the written approval of the Client.
(c) take all security measures required pursuant to Article 32 of the GDPR. An overview of the technical and organizational measures taken by processor are set forth in **Schedule I**.
(d) considering the nature of the processing, assist The Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Clients obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR.
(e) assist The Client in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR considering the nature of processing and the information available to processor.
(f) at the choice of The Client and without any additional costs for The Client, irrevocably delete, remove, or return all the personal data to The Client upon termination of / dissolving this Agreement, expiration of the retention period(s) as defined in the Agreement Summary or at request of The Client and delete existing copies unless Union or other national or local legislation requires storage of the personal data. At the request of The Client, processor shall provide with reasonable evidence of its compliance to irrevocably delete or removal the personal data. Any return of personal data to The Client shall take place in a general acceptable, structured data format by electronic means. If it is not possible to return or irrevocably delete or remove the data, Processor shall immediately inform The Client. In that case processor guarantees that the personal data will be treated confidential and that the personal data will no longer be processed.
(g) make available to The Client, without any additional cost for The Client, all information necessary to demonstrate compliance with the obligations laid down in clause 2 of the Agreement and in general Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by The Client or another auditor mandated by The Client.

3.2 Processor shall not transfer, or otherwise process any personal data outside (a) the European Economic Area or b) those territories in respect of which the European Commission has made a positive finding of adequacy of the protection of personal data, except with the prior written consent of the Client and in accordance with any additional terms the Client may impose on such transfer, e.g., a contract incorporating the EU-Standard Contractual-Clauses. The foregoing provisions of this clause shall apply to any onward transfer from such permitted territories.
3.3 Processor shall immediately inform The Client if, in its opinion, an instruction infringes the GDPR or national or local data protection legislation.
3.4 Processor shall maintain all records required by Article 30 (2) of the GDPR and, to the extent applicable to the processing of personal data on behalf of The Client, make them available to the Client upon request and at no additional cost.
3.5 Processor shall store the personal data no longer than necessary for the purposes as set out in the Agreement Summary.
3.6 Processor shall, if required to do so by European Union or other applicable national and/or local legislation, designate a data protection officer.

4. SUB PROCESSORS

4.1. Where processor engages a Sub processor for carrying out specific processing activities on behalf of the Client, the same data protection obligations as set out this Agreement shall be imposed on the Sub processor by way of a written contract, providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR and all applicable national and/or local legislation.
4.2. Processor shall warrant and guarantee that its Sub processor(s) shall comply with the GDPR and all applicable national and/or local legislation Where the Sub processor fails to fulfil its data protection obligations, processor shall remain fully liable to the Client for the performance of the Sub processor's obligations.
4.3. Processor is only allowed to use Sub processors with the prior approval of the Client. A list of approved Sub processors is set out in Schedule II.

5. NOTIFICATION OF A PERSONAL DATA BREACH

5.1. The Processor shall take all urgent appropriate measures and cooperate with the Client breach response plan to contain the breach, protect the personal data, and inform the Client without undue delay (at least within a timeframe that enables the Client to comply with its (notification) obligations under the GDPR).
5.2. In addition to Article 33 (2) GDPR the notification of processor in case of a personal data breach shall at least:
(a) describe the type and nature of the personal data breach including where possible, the categories and the number of data subjects concerned, and the categories and approximate number of personal data records concerned.
(b) communicate the name and contact details of the data protection officer or other contract point where more information can be obtained.
(c) describe the likely consequences of the personal data breach.
(d) describe the measures taken or proposed to be taken by processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
5.3 Processor shall make its best efforts to assist the Client in fulfilling its obligation to notify the relevant supervisory authority and data subjects of a personal data breach under Articles 33 and 34 of the GDPR.

6. RIGHTS OF DATA SUBJECTS

6.1. Processor shall make its best efforts to assist the Client in fulfilling the Clients obligations under Articles 12 (2) and (3) GDPR to facilitate the exercise of data subject rights under Articles 15 to 22 GDPR. Each party shall carry its own costs.
6.2. Processor shall transfer any received request from data subjects within three days.to the Client.

7. TERM

7.1. The Agreement will govern the relationship between the Parties from the Start Date to the End Date and for any periods of extension or continued performance by the Parties (the "Term").
7.2. Any terms and conditions which are intended by their nature to survive any termination, cancellation, or expiration of the Agreement, amongst others the clauses and paragraphs as set forth in the Agreement Summary, shall remain in full force and effect.
7.3. The Client will have the right to terminate or dissolve the Agreement:
(a) at any time for convenience by providing no less than thirty (30) calendar days' written notice to processor; or
(b) immediately without any liability if the processor becomes unable to perform the services under the Main Agreement or fails to comply with the provisions of this Agreement (including compliance with the GDPR and/or other applicable national or local legislation regarding data protection); or
(c) immediately without any liability in the event that another entity (not being a company under common Control), directly or indirectly, in a single transaction or series of related transactions, acquires Control of processor or all or substantially all of its assets. "Control" for these purposes means the ability to direct the affairs of processor, whether by means of voting or contractual rights or otherwise, and whether directly or indirectly.
7.4. Each party will have the right to terminate the Agreement immediately without any liability in the event that the other party enters into liquidation, goes bankrupt, becomes

unable to pay its debts in the ordinary course of business, pass a resolution for a winding up, has a receiver appointed over all or any significant part of its assets or otherwise becomes insolvent under the laws of the country in which it is incorporated or ceases or threaten to cease to carry on its business.

7.5. If there is a risk of processor going bankrupt, entering liquidation, or passing a resolution for a winding up, processor immediately informs the Client, in order for the Client to decide to timely recover the personal data.

8. LIABILITY AND INDEMNITY

8.1. Processor is responsible for and shall fully indemnify, keep indemnified and hold harmless the Client and its affiliates, and their officers, agents, employees and customers against all liability, losses, costs, claims (including fines and penalties of the supervisory authority) and expenses (including legal expenses) and demands which the Client may incur, howsoever directly or indirectly arising from any failure by the processor and/or its Sub processors to comply with this Agreement and the GDPR.

9. INSURANCE

9.1. Processor shall arrange adequate insurances to cover all liability that might arise under the Agreement and ensure that the insurances are in full force and effect throughout the life of the Agreement.

9.2. The provisions of this clause 8 shall in no way limit the liability of the processor under the Agreement.

9.3. The processor shall supply the Client with evidence of such insurance on demand.

9.4. The processor shall procure that Sub processors are insured to appropriate levels as may be relevant to their services.

10. NOTICES

10.1. Any notice required or permitted to be given by either of the Parties shall be in writing addressed to the other party at the address mentioned in the Contact Details of the Agreement Summary or to such other address as may have been notified by the other party in writing.

10.2. Notwithstanding the provisions of clause 6 of this Agreement, any notice will be properly served if delivered personally or sent by registered mail to the address specified in the Contact Details of the Agreement Summary.

11. ENFORCEABILITY

11.1. If one or more of the provisions of the Agreement is declared to be invalid, illegal, or unenforceable by law, the validity, legality, and enforceability of the remaining provisions contained herein shall not in any way be affected. Each of the Parties shall use its best efforts to negotiate in good faith a legally valid replacement provision, which corresponds in the best possible way with the invalid provision.

11.2. Except in relation to the Affiliates of the Client, it is not intended that any term of this Agreement should be enforceable by virtue of the Contracts (Rights of Third Parties) Act 1999 or the equivalent legislation in the Jurisdiction detailed in the Agreement Summary by any person other than the Client and processor.

12. ENTIRE AGREEMENT

12.1. Parties explicitly declare that this Agreement and the documents referred to herein constitute the entire agreement between Parties and supersedes any prior draft, agreements, undertakings, understandings, conditions, and arrangements, notwithstanding any conflicting order of precedence, of any nature between the Parties, whether or not in writing, in relation to the subject-matter of this Agreement.

13. LAW AND JURISDICTION

13.1. Any contractual or non-contractual obligations arising from or connected with this Agreement shall be governed by and shall be construed in accordance with the law of the Jurisdiction set forth in the Agreement Summary.

13.2. The Parties irrevocably agree that the courts in the Jurisdiction set forth in the Agreement Summary are to have exclusive jurisdiction to settle any dispute which may arise out of or in connection with this Agreement and that accordingly any proceedings arising out of or in connection with this Agreement shall be brought in such courts.

Accepted and agreed.
For and on behalf of the Processor

Signed……..

Name:……..

Position:……..

Date…….

Accepted and agreed.
For and on behalf of the Controller/The Client

Signed……..

Name:……..

Position:……..

Date…….

SCHEDULE I: TECHNICAL AND ORGANISATIONAL MEASURES

This Schedule is an integral part of the Agreement and must be completed and signed by the Parties.
Description of the technical and organisational measures:

Transportation

1. Unless specified otherwise the processor will be responsible for the transportation of the Client files from a designated collection point(s). Ideally the Client will have sealed their files within sealed crates if not Client boxes/files will be loaded in to vans which will be then sealed with serial numbered tags for each collection/return. A photo will be taken of the seal at the beginning and conclusion of each journey. Photos of the seals will be uploaded to the Client Project Folder located within their secure designated Citrix ShareFile cloud portal account created by the Processor. Photos along with other Client Project related matters/logs can be accessed and downloaded by the Client for audit record purposes. Alternatively project related data can be made available via an alternative Client requested method.

Staff

2. All Processor staff involved with the Client projects are DBS cleared. In addition, all staff connected with the Client project are prepared to sign NDA's (Non-disclosure agreements – supplied by the Client) to confirm that all Client files/data will be handled in the strictest confidence.
3. No Processor team members involved with the processing of Client files will be left unattended whilst in the presence of files. The Processors PM (Project Manager) will always remain on-site whilst files are being processed.
4. No Processor team members will be permitted access to mobile phones whilst processing the Client files.

Computers/Systems

5. All PC's involved with the scanning/processing of Client files will automatically screen lock if not used for more than 30 seconds.
6. No PC involved with the scanning or processing of Client files will have internet access.
7. All PC workstations will have passwords reset on a weekly basis. Passwords are randomly generated via the "Norton Password Generator Service" and are at least 8 characters in length containing a combination of alpha, numerical, uppercase, and special characters.
8. If agreed AES 256-bit encrypted USB3 external HDD (Hard Drive(s)) will be used to transfer urgently requested individual scanned files from the scanned files located on the designated Client processing workgroup PC's to the Processors internet connected PC with access to the Citrix ShareFile Portal. Only nominated Client designated users as well as the Processor PM will have access to the Citrix ShareFile Portal. Access to shared urgent files will be removed after 1 x download or 24hrs if not accessed. Once a file has been successfully uploaded to the Citrix ShareFile portal it will be immediately deleted from the external hard drive. Alternatively, the external HDD can be physically couriered to the Clients designated offices, the cost of this additional service is to be borne by the Client unless agreed otherwise in writing.
9. Processed/scanned files are transferred to the Client via AES 256-bit encrypted USB3 external 1Tb HDD (encrypted external hard drives). Each hard drive uses a 6-digit keypad to gain access to the data. The access codes are changed each time the hard drives are used and are to be generated by the Client. The external hard drives used to transport scanned files are rotated with each drop off/collection of The Client files.

Citrix ShareFile Cloud Portal

10. Where agreed with the Client, the Processor will make urgent/sample files available to the Client via the Citrix ShareFile Cloud Portal. Files are kept secure during transfer using SSL/TLS encryption protocols.
11. Whilst in the cloud, storage of files is kept safe using AES 256-bit encryption. This process is used for files both at rest and in transit.
12. Files shared via the Citrix ShareFile portal will be encrypted and password protected prior to sharing.
13. All activity related to both the Client files as well as designated users with file/cloud access is recorded within a secure log. Activity such as file access, shares, downloads, user logins and user IP addresses are permanently logged.
14. Access as well as share privileges for The Client designated users (if any) are to be agreed and set-in place prior to any The Client file activity.
15. MFA (Multi-factor authentication) is to be set for all user accounts with access to The Client stored data.

Email Communications

16. The Processor will communicate project details with the Client via the secure Microsoft Outlook 365 platform where possible.
17. No sensitive data relating the Clients project will be made available via normal Microsoft email protocols.
18. If agreed with the Client, sample, as well urgently required files will be made available via the Citrix ShareFile email portal. All emails sent via the Citrix ShareFile platform will be encrypted along with password protected. Only the designated Client user will have access to Citrix ShareFile generated email file shares.
19. All Citrix ShareFile file shares will be subject to both the number of times a file may be download as well as an expiry availability period of 24hrs unless agreed otherwise by the Client.
20. If agreed with the Client all project related data such as logs, spreadsheets along with photos of security seals will be made available via the Citrix ShareFile portal.

Availability and Resilience

21. All Client scanned data will be backed up at the end of each working day and copied to an AES 256-bit encrypted USB3 external HDD (encrypted external hard drives). The PM will collect the Hard Drive at the end of each day and store it offsite within a secure SIL wall mounted electronic fireproof safe.

Retention/Deletion Controls

22. Upon completion of the Client project all PC Hard Drives involved with the Clients project will be handed to the Client so that they may be securely destroyed. Alternatively, the Processor may securely destroy the Hard Drives if instructed by the Client to do so, the cost of this additional service is to be borne by the Client unless agreed otherwise in writing.

Environment

23. The Processors offices accommodate Client PC workgroups for each project with no internet access. The lack of internet access prevents any potential external threat of data being accessed.
24. Each Client project is run within its own standalone PC workgroup with no access to other Client project workgroups. No cross contamination of Client data is possible.
25. Access to the Processor scanning area is via a Libo 125khz electronic door entry system. Only Processor team members associated with the Client project are allocated access codes. All access is recorded via the keypad logs plus 24hr recorded CCTV.
26. No unauthorised staff members will have access to either the Client Files or the workstations scanning them.
27. Either the PM or a senior member of the Processors team associated with the Clients project will always remain onsite whilst the Clients files are being processed.
28. No other Client files/projects will be processed within the same working area as the Clients project files.
29. Staff members not connected with the Client project will be denied access to both the Clients physical files as well as the workstations used to scan/process the Clients files.
30. All staff activity connected with the Client project will be monitored by the Processors senior staff/partners.
31. CCTV (Sricam) monitoring of the Client scanning area will be recorded 24hrs per day, 7 days per week for the duration of the project.
32. Each scanning station will record the scanning operator responsible for scanning each Client file.
33. No Client files will be left unsecured when the Processors staff are not onsite. When scanning is completed each day files will be returned to their secure contained storage areas.
34. The Storage facility is gated, alarmed, and has 24hr CCTV.

Notification Of A Personal Data Breach

35. The Processor shall take all urgent appropriate measures and cooperate with the Client a breach response plan to contain the breach, protect the personal data, and inform the Client without undue delay (at least within a timeframe that enables the Client to comply with its (notification) obligations under the GDPR).
36. In addition to Article 33 (2) GDPR the notification of processor in case of a personal data breach shall at least: describe the type and nature of the personal data breach including where possible, the categories and the number of data subjects concerned, and the categories and approximate number of personal data records concerned. communicate the name and contact details of the data protection officer or other contract point where more information can be obtained.
37. Describe the likely consequences of the personal data breach.
38. Describe the measures taken or proposed to be taken by processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
39. Processor shall make its best efforts to assist the Client in fulfilling its obligation to notify the relevant supervisory authority and data subjects of a personal data breach under Articles 33 and 34 of the GDPR.

SCHEDULE II: APPROVED SUB PROCESSORS

Within the framework of compliance with the contractual obligations' processor shall be entitled to use the following Sub processors:

[Please complete the following table after a corresponding checking of the Sub processors]

#	Name	Address	Area of use
1	*Not applicable*		
2			

SCHEDULE III: PROCESSING OF PERSONAL DATA

If the given options are not sufficient, please complete the required information by using the 'Others' option.

SUBJECT MATTER	Scanning of ????	
NATURE OF PROCESSING	Collection Recording Structure Modification Storage **Others**: Scanning of documents	Comparison ☐ Restriction ☐ Erasure / Destruction ☐ Retrieval ☐ Consultation ☐ Disclosure by transfer / Communication
PURPOSE OF THE PROCESSING	☐ The Client, accounting, fiscal and administrative management Payroll Management Provision of financial solvency and creditworthiness services Insurance and economic-financial services Pension Plan Advertising and commercial research Guide/repertory of electronic communication services Provision of electronic certification services Associational, cultural, diversionary, sport and social activities management Education Sanitary control and management Private security **Others**: ????????.	Video surveillance Human resources Occupational risk prevention Fulfilment/Failure of monetary obligations Profiling Provision of electronic communication services E-commerce Political parties, unions or Church associates or members Management Social assistance management Epidemiology investigation and similar activities Clinical history Buildings security and access control Statistical, historical, or scientific purposes Dispute management IT services (e.g., PaaS, SaaS, IaaS) (e.g., hosting of a website, off-line data processing, cloud services, or similar)
TYPE OF PERSONAL DATA	Identification data National identification number (or equivalent) Personal characteristics Academic & professional Commercial information Living habits Family composure Social circumstances Employment details Economic, financial or insurance specifics Goods and services transactions Special categories of personal data Financial specifics Profession and employment Payroll data Information about absence and leave. Payroll data Performance data Other data: any data contained in the employee files.	
CATEGORY OF DATA SUBJECTS	Employees Consumers Customers (contact persons/representatives) Suppliers (contact persons/representatives) Associates or members. Owner or tenant **Others**:	Contact person. Parents or guardian Legal representative Job applicants Beneficiaries Public Officers Students

'