

## Standard Terms & Conditions

### 1. DEFINITIONS

1.1 Throughout this Agreement the following terms will mean:

**“Agreement”** means this Agreement for the provision of Services as defined by this document in its entirety.

**“Client”** means the company that ICTRAM provides the Services.

**“Confidential Information”** means all information relating to either party in respect of business or negotiations under the terms of this Agreement.

**“Data Controller”** has the same meaning as Controller within Data Protection Laws.

**“Data Processor”** has the same meaning as Processor within Data Protection Laws.

**“Data Protection Clauses”** has the same meaning as per Schedule 1.

**“Data Protection Laws”** means the GDPR, the Data Protections Act 2018, The Privacy and Electronic Communications (EC Directive) Regulations 2003, any other applicable law relating to the processing, privacy and/or use of Personal Data, any laws which implement any such laws and any laws that replace, extend, re-enact, consolidate, or amend any of the foregoing.

**“Effective Date”** means the date that this Agreement is entered into by both parties

**“Force Majeure”** means an event which is beyond the control of either Party, or which prevents either Party from complying with the terms of this Agreement. Such events may include, but not be limited to, acts of God, such as fires, explosions, floods, and/or riots, strikes or general disorder or acts of terrorism. It is the responsibility of the affected Party to inform the other Party, in writing, within five (5) working days that an event of Force Majeure has taken place and give details of such an event and how the situation will be rectified.

**“GDPR”** means the General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time).

**“ICTRAM”** means ICT Reverse Asset Management Limited.

**“Intellectual Property Rights”** means copyright, designs, patents, confidential information, and trademarks.

**“Laws”** means all laws, legislation, and regulations applicable to the Services carried out under the terms of this Agreement and are binding on both Parties.

**“Party”** or **“Parties”** means either the Client and/or ICTRAM.

**“Premises”** means the premises to where ICTRAM will transport the Products, in order for the Services to be undertaken

**“Price”** means the price(s) as outlined in the Statement of Work.

**“Processing”** has the same meaning as set out in the Data Protection Laws

**“Products”** means the assets upon which ICTRAM will perform the Services on behalf of the Client and are detailed in the SOW and such other assets as the Parties hereto may from time to time agree to in writing.

**“Services”** mean the services (including any part thereof) to be performed by ICTRAM as agreed with the Client.

**“Specifications”** means the technical specifications and descriptions of the Products including design and material composition and, but without limitation, details of hazardous materials or other potential hazards.

**“Statement of Work”** means the Statement of Work (SOW) provided to the Client. The SOW confirms, without limitation, the scope of the Services provided by ICTRAM.

**“Sub-processor”** means any person (including any third party but excluding an employee of ICTRAM) appointed by or on behalf of ICTRAM to Process Personal Data on behalf of Customer or any Customer Affiliate in connection with this Agreement.

**“Working Days”** shall mean Monday to Friday from 8.15am to 5pm but shall exclude all United Kingdom Bank Holidays and Public Holidays.

1.2 The headings to the Clauses and Schedules of this Agreement will not affect its construction.

## 2. APPOINTMENT

2.1 In appointing ICTRAM, the Client relies on ICTRAM's undertaking that ICTRAM has in place the resources and expertise to carry out the Services to the standards specified within this Agreement.

2.2 The Parties agree that, subject to Clause 7 (Confidentiality), the terms of this Agreement do not restrict ICTRAM from providing the same or similar services to other parties.

2.3 Client and any of its Subsidiaries may directly procure services under this Agreement from ICTRAM by entering into a Statement of Work in the name of the relevant Client entity. In the event a Statement of Work is entered into by a Subsidiary of Client, the terms of this Agreement shall apply to such Statement of Work as if such terms had been entered into between the relevant Subsidiary of Client and ICTRAM, and any reference to Client in this Agreement will be deemed to be a reference to the relevant Subsidiary named in the Statement of Work.

## 3. ICTRAM'S OBLIGATIONS

3.1 ICTRAM will perform the Services required by the Client and in accordance with the SOW.

3.2 ICTRAM will use all reasonable endeavours to complete the Services to a standard set out in the SOW using best industry practices and in accordance with all governing legislation and laws.

3.3 ICTRAM undertakes to ensure it holds and maintains all necessary industry accreditations required by current legislation and laws pertaining to the correct performance of the Services the details of which are set out on the ICTRAM website and as updated from time to time.

3.4 ICTRAM will undertake the Services using its own employees and/or subcontractors who meet the standards required to carry out the Services.

3.5 In the event that ICTRAM needs to make changes to the Services or the provision thereof due to amendments in the law or legislation governing the Services, then ICTRAM will notify the Client in writing and the Client's approval to such changes will not be unreasonably withheld. If such approval is not forthcoming then ICTRAM retain the right to terminate this Agreement without notice.

3.6 The Client undertakes to ensure that ICTRAM are not prevented or hindered from carrying out the Services. If such an event should occur then ICTRAM will promptly advise the Client of the circumstances and ICTRAM will not be penalised for any failure or delay in carrying out the Services.

3.7 In order to discharge its obligations under the Services ICTRAM may need password from the Customer for the Products. In the event that, after a request for the password, none is provided to allow ICTRAM to access the Product to perform the Services within 30 days ICTRAM reserve the right to deal with the Product in the most efficient manner available.

3.8 ICTRAM are able to offer a range of logistics services to reflect customer budget and security requirements. Unless otherwise requested in writing ICTRAM will arrange the most cost-effective logistics service for each customer. This will include a single driver and could include the use of shipping hubs, multi-point collections and basic courier services.

3.9 All handsets are IMEI checked with national crime database CheckMEND; [www.checkmend.com](http://www.checkmend.com). Any item which is IMEI barred will be rejected and disposed of by ICTRAM in an environmentally sound manner in line with ISO 14001 and the EU Waste Electrical and Electronic Equipment (WEEE) Directive. No price shall be payable in respect of any such Products.

3.10 Blancco mobile edition is applied to all working SMART Phones received by ICTRAM. Only handsets that can be data erased by Blancco mobile edition are subject to indemnity insurance provided by the third-party supplier.

3.11 Any Products with Hard Drives, will be fully wiped and all data destroyed using Blancco (this process will be performed until it is 100% successful to a base line standard of Information Assurance Level 5) any Hard Drives that after stringent testing have not been fully cleansed will be permanently destroyed.

3.12 Other data bearing assets are handled as below:

On client site		Media Type	At processing facility	
Reuse	Destruction		Reuse	Destruction
CPA Blancco 6.1.70 / 7.2.0	eDR Disk Crusher & EvaShred EV30E	Magnetic Hard Disk Drives	CPA Blancco 6.1.70 / 7.2.0	eDR Disk Crusher & EvaShred EV30E
Blancco 6.1.70 / 7.2.0	eDR Disk Crusher & EvaShred EV30E	Solid State Hard Drives	Blancco 6.1.70 / 7.2.0	eDR Disk Crusher & EvaShred EV30E
Blancco 4.10 Mobile	eDR Disk Crusher & EvaShred EV30E	Smart Phones	Blancco 4.10 Mobile	eDR Disk Crusher & EvaShred EV30E
CPA Blancco 6.1.70 / 7.2.0	eDR Disk Crusher & EvaShred EV30E	Hybrid Disk Drives	CPA Blancco 6.1.70 / 7.2.0	eDR Disk Crusher & EvaShred EV30E
	Shred to 12mm	Routers (Wired and Wireless)	Reset to factory default settings contact vendor for appropriate sanitisation procedure	Shred to 12mm
	Shred to 12mm	Printers, Copiers and Multi-function devices	Reset to factory default settings contact vendor for appropriate sanitisation procedure	Shred to 12mm
	Shred to 12mm	Magnetic Tapes		Shred to 12mm
	Shred to 12mm	Optical Disks		Shred to 12mm
	Shred to 12mm	Removable Media such as USB	Blancco Flash Media	Shred to 12mm
	Shred to 12mm	Paper / Microforms		Shred to 12mm

#### 4. CLIENT'S OBLIGATIONS

4.1 The Client will undertake to comply with the terms contained in the SOW in a timely manner and, without prejudice, the Client will at all times:

4.1.2 provide ICTRAM with correct instructions and directions relative to carrying out the Services;

4.1.3 respond promptly to requests for information and/or directions as maybe requested by ICTRAM from time to time;

4.1.4 promptly advise ICTRAM in the event that the Client becomes aware of any problems or potential problems which may impact on the successful undertaking of the Services;

4.1.5 ensure that ICTRAM are not obstructed from undertaking the Services and that the health and safety of the ICTRAM employees or subcontractors is not placed in jeopardy;

4.1.6 ensure that any action or lack of action by the Client does not increase the cost to ICTRAM of providing the Services;

4.1.7 obtain and maintain in force all licenses, approvals, registrations and qualifications required to enter into this Agreement;

4.1.8 comply with all applicable Laws.

4.2 The Client will not include products unless stipulated in the SOW without the prior written approval of ICTRAM. If non agreed Products are included their collection will not amount to acceptance by ICTRAM. If ICTRAM agree to include such items, it is understood by both parties that this may include an additional cost to the Client.

4.3 The Client undertakes to advise ICTRAM in writing and in advance of the Services of any hazardous waste or other potential hazards which may be contained in the Products.

4.4 ICTRAM may, from time to time, request a Specification of the Products if the Client advises that the Products contain hazardous substances. If the Client is unable to provide such Specification then ICTRAM may undertake testing of the Products and the Client will meet all costs which may be incurred if such testing is undertaken. ICTRAM will not be in breach of this Agreement if it rejects Products where the Client has not provided a Specification or allowed ICTRAM to carry out testing for hazardous substances.

#### 5. DELIVERY OF THE PRODUCTS

5.1 ICTRAM will arrange collection of the Products from addresses stipulated in advance by the Client.

5.2 Unless otherwise stated in the SOW, the Client will be responsible for preparing and packaging the Products.

5.3 Unless otherwise agreed, the weight of each consignment of the Products as recorded by ICTRAM will be conclusive evidence of the weight of the Products received by ICTRAM.

5.4 ICTRAM's signature, given on any delivery note, or other documentation, presented for signature in connection with delivery of the Products, is evidence only of the collection being carried out. In particular, it is no evidence that the correct quantity or number of Products has been delivered or that the Products delivered are in good condition or of the correct quality.

#### 6. RISK AND TITLE

6.1 ICTRAM will bear the risk of loss or damage to the Products during transportation and whilst the Products are located at the Premises.

6.2 The Client will bear the risk of loss or damage to the Products while the products remain at the Client's

facilities or are being transported by the Client.

6.3 The Client hereby warrants that it holds full title to the Products and that no third party has any interest in the Products.

6.4 Title to the Products will transfer to ICTRAM on delivery.

## 7. CONFIDENTIALITY

7.1 Both Parties agree:

7.1.1 not to disclose or make public any aspects regarding this Agreement or the negotiations between the Parties;

7.1.2 not to disclose any Confidential Information to any third party other than to employees involved in the implementation of this Agreement.

7.2 Each Party will ensure that its employees, agents and subcontractors maintain the Confidential Information in strictest confidence and will not use such information for anything other than the implementation of this Agreement.

7.3 If it is deemed necessary to divulge Confidential Information to a third party the Parties must agree to this in writing before such information is disclosed.

7.4 Each Party warrants that it has not published or disclosed any Confidential Information relating to this Agreement prior to the Effective Date.

7.5 Each Party agrees that the provisions of this Clause 7 in its entirety will remain in force after the termination of this Agreement for a minimum period of 1 year.

## 8. MANAGEMENT OF SERVICES

8.1 ICTRAM and the Client undertake to manage and review the Services in accordance with the terms of the SOW.

8.2 ICTRAM and the Client will nominate a key representative who will be the main contact for the other Party and who will be authorised to make decisions to ensure the implementation of this Agreement.

8.3 ICTRAM agrees that during the term of this Agreement, subject to 7 (seven) working days' notice, it will permit the Client's designated employees' access during regular office hours to the Premises to view the systems, procedures, records and books maintained by ICTRAM in support of this Agreement. ICTRAM retain the right to withhold any information which it deems Confidential. ICTRAM will provide reasonable assistance to any authorised person(s) undertaking the review.

## 9. CHANGES TO THE SERVICES

9.1 During the term of this Agreement either Party may request in writing a variation to part or parts of the Services.

9.2 Both Parties will investigate the requested variation and will make written recommendations within 14 (fourteen) working days of the first notification of the requested variation together with a quotation of any additional costs involved.

9.3 Neither Party will unreasonably withhold its agreement to the proposed variation to the Services.

9.4 Notwithstanding the above, if ICTRAM is unable to comply with the variation to the Services it will advise the Client in writing within 21 (twenty one) working days. In such circumstances the Client may source the services of a third party to cover the variation to the Services.

## 10. FORCE MAJEURE

10.1 Neither Party will be in breach of this Agreement or liable to the other Party in any manner whatsoever for failure or delay in performing its obligations under this Agreement due to Force Majeure.

10.2 If either Party is unable to adhere to its obligations under this Agreement due to Force Majeure, then it will give the other Party notice in writing within 10 (ten) working days of becoming aware of the Force Majeure.

10.3 Neither Party will be entitled to payment from the other Party in respect of additional costs incurred due to the Force Majeure.

## 11. LIMITATION OF LIABILITY

11.1 Nothing in this Agreement shall limit or exclude the ICTRAM's liability for:

11.1.1 death or personal injury caused by its negligence, or the negligence of its personnel, agents or subcontractors;

11.1.2 fraud or fraudulent misrepresentation; and

11.1.2 breach of the terms implied by section 2 of the Supply of Goods and Services Act 1982 (title and quiet possession) or any other liability which cannot be limited or excluded by applicable law.

11.2 Subject to 12.1, ICTRAM shall not be liable to the Client, whether in contract, tort (including negligence), for breach of statutory duty, or otherwise arising under or in connection with this agreement for:

11.2.1 loss of profits;

11.2.2 loss of sales or business;

11.2.3 loss of agreements or contracts;

11.2.4 loss of anticipated savings;

11.2.5 loss of use or corruption of software, data or information;

11.2.6 loss of or damage to goodwill; and

11.2.7 any indirect or consequential loss.

11.3 Subject to 12.1 ICTRAM's total liability to the Client, whether in contract (including negligence), for breach of statutory duty, or otherwise arising under or in connection with this agreement shall be limited to the greater of £250,000 and One Hundred per cent (100%) of the average annual charges (calculated by reference to the Charges in successive 12-month periods from the Services Start Date paid by the Client under this Agreement.

11.4 The conditions implied by sections 3,4, and 5 of the Supply of Goods and Services Act 1982 as to the fullest extent permitted by law, excluded from this agreement.

11.5 During the Term of this Agreement ICTRAM shall maintain at its own expense the insurances governing the Services

11.5.1 public liability insurance in the sum of £5,000,000 per claim;

11.5.2 products liability insurance in the sum of £5,000,000 per claim and in the aggregate per annum;

11.5.3 professional indemnity in the sum of £5,000,000 per claim;

11.5.4 employer liability insurance in the sum of £10,000,000 per claim.

## 12. TERMINATION

12.1 Either Party may serve written notice of immediate Termination if the other Party:

12.1.1 is in breach of the terms of this Agreement and where the breach is capable of remedy but the Party fails to undertake such remedy within 30 (thirty) working days from written notice of the breach by the other Party;

12.1.2 becomes bankrupt, insolvent, enters into any arrangement with its creditors, appoints a receiver or liquidator and/or receives a winding up order;

12.1.3 is found to have entered into unlawful practices;

12.2 The rights to terminate this Agreement given by this Clause will not prejudice any other right or remedy by either Party in respect of any breach of the terms of this Agreement.

12.3 ICTRAM may invoice the Client for any Services performed under this Agreement up to and including the date of termination and the Client will pay such invoice under the terms of this Agreement.

12.4 The Parties will mutually agree as to how to dispose of any Products which remain unprocessed on the date of termination. In the event that the Parties are unable to reach such an agreement then ICTRAM will return the Products to the Client at the Client's expense.

12.5 Upon termination each Party will promptly return to the other Party all documentation or materials which incorporates the other Party's Intellectual Property Rights or Confidential Information.

## 13. ENTIRE AGREEMENT

This Agreement contains all the terms to which the Parties have agreed to in relation to the Services as defined in the SOW. No other promises or undertakings beyond the terms of this Agreement have been made by either Party.

## 14. SUBCONTRACTING

14.1 ICTRAM may subcontract all or part of its obligations as defined by this Agreement. ICTRAM will however remain liable for such obligations under this Agreement and will be responsible for any failure of the subcontractor.

14.2 ICTRAM may subcontract all or part of any mobile device consignments to its Asset Disposal Information Security Alliance (ADISA) approved downstream specialist.

## 15. INVALIDITY

If any part, clause or condition of this Agreement is found by a competent legal authority to be illegal, invalid or unenforceable and if modification fails to remedy the situation, then it will be struck from this Agreement.

## 16. WAIVER

16.1 Any failure or delay by either Party to exercise any right, power or remedy under this Agreement will not impair any such right, power or remedy nor operate a waiver of it.

16.2 Any waiver of a breach or default under any of the terms of this Agreement will not affect other terms of this Agreement.

## 17. DATA PROTECTION



17.1 Each Party will be responsible for compliance with all relevant Laws relating to the Processing and security of data.

17.2 The Customer, as Data Controller has chosen ICTRAM to be its Data Processor reliant upon the guarantees in respect of the technical and organisational security measures governing the Processing to be carried out by ICTRAM and has taken reasonable steps to ensure compliance with those measures.

17.3 The Customer, as Data Controller using ICTRAM as its Data Processor, confirms that the Processing is carried out under this Agreement and the SOW. ICTRAM understands and acknowledges that, to the extent that performance of its obligations under this Agreement and the SOW involves or necessitates the processing of Customer Personal Data, it shall process such Customer Personal Data only for such purpose and only in accordance with the express written instructions of Customer including with respect to any transfers of Customer Personal Data to a country outside the United Kingdom.

17.4 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 of varying likelihood and severity for the rights and freedoms of natural persons, ICTRAM shall in relation to the Personal Data implement all such technical and organisational measures necessary or appropriate to preserve the security and confidentiality of such Personal Data to which it has access and protect such Personal Data from accidental or unlawful loss, destruction, alteration, damage and unauthorised access or disclosure. In assessing the appropriate level of security, ICTRAM shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach

17.5 ICTRAM shall notify Customer without undue delay upon it becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow it to meet any obligations to report or inform a Supervisory Authority and Data Subjects of such Personal Data Breach under Data Protection Laws.

17.6 ICTRAM shall give Customer prior written notice of the appointment of any new Sub-processor, including full details of the Processing to be undertaken by such Sub-processor. Customer may object in writing to the proposed appointment, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution.

17.7 ICTRAM shall co-operate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation, and remediation of each Personal Data Breach.

17.8 With respect to each Sub-processor, ICTRAM shall:

17.8.1 before the Sub-processor first Processes Customer Personal Data, carry out reasonable due diligence to ensure that the Sub-processor is capable of providing the level of protection for Customer Personal Data required by this Agreement and SOW.

17.8.2 ensure that the arrangement between ICTRAM and the Sub-processor, is governed by a written contract which shall include the same data protection obligations as those set out in this Agreement and meet the requirements of Article 28(3) of the GDPR or equivalent provisions of any other Data Protection Law; and

17.8.3 remain responsible for its compliance with the obligations set out in this Agreement and for any acts or omissions of the Sub-processor that cause ICTRAM to breach any of its obligations under this Agreement and SOW.

## 18. VARIATION

No variation of the terms of this Agreement will be valid unless agreed in writing by duly authorised representatives of both Parties.

## 19. RELATIONSHIP OF PARTIES

Nothing in this Agreement will be deemed to indicate a joint venture or partnership between the Parties.

## 20. NOTICES

20.1 Any and all communications, notices or other matters, from either Party, which may affect the terms of this Agreement must be submitted in writing and delivered by hand, first class post or Special Delivery to the recipient's registered address.

20.2 Such communication will be deemed to have been received when delivered by hand during standard office hours, by signed receipt when submitted by Special Delivery or within 5 (five) working days when despatched by first class post.

## 21. RESOLUTION OF DISPUTE

21.1 Where dispute or differences arise between ICTRAM and the Client in respect of this Agreement then the Parties will endeavour to resolve such dispute by working together in good faith without recourse to formal proceedings.

21.2 If the key representatives are unable to resolve the dispute or differences within 30 (thirty) working days then either Party may refer the matter to its senior management.

21.3 Neither Party will commence formal proceedings until all reasonable efforts have been made to resolve the dispute or differences.

21.4 Nothing in this Agreement will prevent either Party carrying out formal proceedings in order to protect Intellectual Property Rights or Confidential Information.

21.5 If the Parties are unable to resolve the dispute or differences then they may progress to mediation through formal proceedings. Neither Party may unreasonably withhold its agreement to such proceedings.

21.6 If either Party refuses to comply with formal proceedings and of the dispute or differences are not resolved within 60 (sixty) working days then either Party may commence proceedings in accordance.

## 22. BRIBERY PREVENTION MEASURES

22.1 ICTRAM hereby agrees that:

22.1.1 it will comply with applicable law, and with all regulations, codes and sanctions that have legal effect relating to anti-bribery and anti-corruption including but not limited to the UK Bribery Act 2010 (the "Anti-Bribery Law");

22.1.2 it will comply with its anti-bribery policy as may be amended from time to time;

22.1.3 it will procure that any person who performs or has performed services for or on its behalf ("Associated Person") in connection with this Agreement complies with applicable Anti-Bribery Laws;

22.1.4 it has and will maintain in place effective accounting procedures and internal controls necessary to record all expenditure in connection with this Agreement;

22.1.5 from time to time, at the reasonable request of the Client it will confirm in writing that it has complied with its obligations under this Clause 22 and will (subject to confidentiality restrictions) provide any information reasonably requested by the Client in support of such compliance;

22.1.6 it shall notify the Client as soon as practicable of any breach of any of the obligations contained within this Clause 23 of which it becomes aware.

Breach of any of the obligations in this Clause 22 shall be deemed to be a material breach of this Agreement.

## 23. GOVERNING LAW

This Agreement and any non-contractual obligations arising out of or in connection with this Agreement shall be governed by and shall be construed in accordance with the laws of England and Wales.

## Schedule 6

### DATA PROTECTION PROCESSING CLAUSES

The following Personal Data Protection Processing Clauses shall be considered as an integral part of the Vendor Service Agreement between [THE CLIENT] (“Controller”) and [ICTRAM], (“Service Provider” or “Processor”).

#### 1. Definitions

- a. “Data Protection Laws” means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any country within EEA, including GDPR Legislation
- b. ‘Data Subject’ mean any individuals from whom The Client collects, uses and/or processes Personal Data for their business purpose. **Explanation:** list includes employees, clients, client customers, agents, contractors
- c. ‘Data Transfer Agreement’ means such data transfer agreements between the Parties based on the model clauses pursuant to Decision 2010/87/EU and/or Decision 2002/16/EC), as applicable, of the European Commission
- d. ‘GDPR Legislation’ means the General Data Protection Regulation ((EU) 2016/679) (“GDPR”) unless and until GDPR is no longer directly applicable, any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the jurisdiction relevant to the Agreements and any successor legislation to GDPR or such national implementing laws, regulations and secondary legislation
- e. ‘EEA’ means the European Economic Area
- f. ‘Technical and Organisational Security Measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing
- g. “Personal Data” means any data or data related to EU residents, as defined under GDPR Legislation
- h. “Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

Controller and Processor shall comply with all applicable requirements under GDPR Legislation. The terms and conditions agreed further in this document is in addition to, and does not relieve, remove or replace, a party's obligations under the GDPR Legislation

#### 2. Processing

- A. Process Personal Data only on the written instructions of the Controller unless the Processor is required by the Applicable Laws. Where the Processor is relying on Applicable Laws, before performing such processing it shall notify the Controller unless those Applicable Laws prohibit the Processor from so notifying the Controller.
- B. Processor shall immediately inform Controller if in its opinion an instruction given by Controller breaches any Applicable Data Protection Laws.
- C. Both Controller and Processor, prior to any such processing shall set out the scope, nature and purpose of processing, the duration of the processing and the types of personal data (as defined in the GDPR Legislation) and categories of Data Subject in the template identified as **Annex 1**

3. **Records of processing Activities**

- A. Processor must keep records of its processing activities performed on behalf of the Controller, as identified in **Annex 2** of this Agreement.

4. **Sub-processing**

- A. Sub-processing shall be authorised in advance, by Controller through either a general or a specific written authorization. Where Personal Data is processed by sub-contractors the Processor shall:
- a. not authorize any third party and/or subcontractor to process the Personal Data ("sub-processor") other than with the prior written consent of the Controller and:
  - b. remain fully liable to the Controller for any failure by a sub-processor to fulfil its obligations in relation to the processing of any Personal Data; and the use of any sub-processor being otherwise in accordance with this clause.
- B. The Controller has the right at any time to demand from Processor full details of the processing to be undertaken by the proposed sub-processor and a copy of the contract between the Processor and the sub-processor.
- C. The Processor must ensure that the contract between Processor and sub-processor enforce obligations similar to the contract agreed between Controller and Processor, including the clauses agreed here, mandating legal mechanism to ensure an adequate level of protection of the Personal Data transferred, including execution of EU Model Contractual Clauses prior to any such processing.
- D. In case the Controller grants a general authorization to sub-processing Personal Data, the Processor shall inform the Controller of any intended changed concerning the addition or replacement of sub-processors, giving the Controller the opportunity to object.
- E. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

5. **Confidentiality**

- A. Where Personal Data is processed by the Processor, its agents, subcontractors or employees, the Processor shall, and shall procure that its agents, sub-contractors, and employees to:
- a. take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Personal Data, as strictly necessary to perform the Services in the context of that individual's duties to the Processor, ensuring that all such individuals.
  - b. are informed of the confidential nature of the Personal Data.
  - c. have undertaken appropriate training in relation to Personal Data Protection.
  - d. are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.
  - e. are aware of the Processor 's obligations in relation to data protection under these clauses.

6. **Security**

- A. Processor, including its agents, subcontractors, employees, shall implement appropriate technical and organisational security measures (more fully identified in **Annex 1**) to ensure a level of security commensurate with the risks associated with the processing, such measures to be appropriate in particular to protect against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to the Personal Data.

7. **Data Subjects Rights**

- A. Processor shall promptly notify Controller upon any request received from Data Subject and assist Controller with requests to exercise Data Subject rights, including but not limited to the right to access and the right to erasure.

8. **Personal Data Breach**

- A. Processor shall notify Controller without undue delay and in any case not later than 24 hours upon becoming aware of a Personal Data Breach affecting Personal Data belonging to Controller, provide Controller with sufficient information to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- B. Processor shall co-operate with Controller or its affiliates, subsidiaries and take such reasonable steps as are directed by Controller to assist in the investigation, mitigation, and remediation of each such Personal Data Breach
- C. Reporting of Personal Data Breaches shall be emailed to The Client's contact within ICTRAM's CRM system describing the Personal Data Breach in terms of who and how many data subjects are affected, where when and how it occurred, which measures have been taken already to stop the breach and mitigate its effects.

9. **Data Protection Impact Assessments**

- A. Taking into account the nature of processing and information available to Processor, Processor shall assist Controller in cases a Data Protection Impact Assessment shall be carried out, wherever applicable.

10. **Cooperation with Data Protection Authorities**

- A. Where applicable, Processor are required to cooperate, on request with Data Protection Authorities in the performance of their tasks.

11. **Availability of Information**

- A. Upon written request of the Controller, the Processor will undertake its commercially reasonable efforts to make available to the Controller all information necessary to demonstrate compliance with

its obligations regarding data protection as explicitly set out in these clauses or by applicable laws and allow for and contribute to audits, including inspections, conducted by the Processor or another auditor mandated by the Processor.

## 12. **Deletion of Existing Personal Data**

- A. Where Personal Data is processed by the Processor, its agents, subcontractors or employees, the Processor shall, and shall procure that its agents, subcontractors, and employees to:
- a. ensure that any IT systems used in the context of performance of these clauses, including any backup systems, allow the erasure or deletion of specific Personal Data, and put in place measures to fully implement any erasure or deletion request within the timeframe required by Controller.
  - b. upon termination for any reason of the provision of Services, cease processing the Personal Data immediately, except for the safe storing. Thereafter, at the Controller's option, either return, or delete from its systems (so that such Personal Data cannot be recovered or reconstructed), the Personal Data and any copies of it or of the information it contains, including any Personal Data in hardcopy format and the Processor shall confirm in writing to the Controller that this clause has been complied with in full.

## **Annex 1**

### **1. Scope**

Secure collection of IT, communication and data bearing assets, Wiping/overwriting of data residing in the data bearing devices of the IT and communication assets, Secure destruction of the data bearing devices which cannot be wiped, Provision of reports and Management information of devices treated.

### **2. Nature**

Will be carried out within European Economic Area ('EEA') or within a Member State of EEA.

### **3. Purpose of processing**

Provision of ICT Reverse Asset Management and data destruction service.

### **4. Duration of the processing**

The agreement is authorised for three years from date of signature where it shall terminate automatically without notice. With regards to duration of processing of data bearing assets, this shall be determined by the associated DIAL completed.

DIAL 1: Booked into CORE on day of receipt, Individually tracked by addition of unique identifier and data sanitisation complete within 45 days.

DIAL 2: Booked into CORE on day of receipt, Individually tracked by addition of unique identifier and data sanitisation complete within 20 days.

### **5. Types of personal data**

As indicated in the DIAL (Data Impact Assurance Level) completed for the service provision, at least comprising data that is residing on the IT and communication assets e.g., Name, email address, telephone number, Employee/HR Data, date of birth, online identifiers, and location data such as IP addresses, mobile device IDs.

#### **6. Categories of data subject**

As indicated in the DIAL (Data Impact Assurance Level) completed for the service provision, at least comprising:

- o Customers
- o Potential Customers
- o Subscribers
- o Employees
- o Suppliers

#### **7. Transfer of Personal Data outside of the EEA**

Not Applicable.

#### **8. Technical and organisational measures**

Encryption, Physical security (premises are protected by CCTV. Control access to premises, supervise visitors), disposal of IT assets, log in/password protection for access, reporting on IT assets e-wasted, Staff training/certification on the protection of personal data.

### **Annex 2**

#### Records of Processing

- a. name and contact details of the Processor, Controller, and respective data processing officer, if applicable.
- b. categories of processing carried out on behalf of each controller.
- c. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards; a description of the Technical and Organisational Security Measures.



### Issue Change/Review Dates

Issue	Description of Change	Date of Issue
v1.0	Initial issue	21/05/2018
V1.0	Reviewed	05/11/2019
V1.0	Reviewed	04/02/2021
V1.1	Reviewed and Schedule 1 added	18/11/2021
V1.2	Updated to reflect ADISA amends	24/03/2022
V1.3	Updated to reflect ADISA criteria	13/12/2022
V1.4	Reviewed and formatting amended	20/03/2023
V1.5	Blancco version update	15/04/2023
V1.6	Blancco version update	12/12/2023
V1.7	Blancco version update	02/01/2024
V1.8	Blancco version update	10/02/2024
V1.9	Addition of Genesis Repair and Erasure, format amend	09/04/2024
V2.0	Addition of Phonecheck as Smart Phone erase. Shred from 12mm to 16mm	01/07/2024
V2.1	Blancco version update	21/01/2025