Contract Template

<client name>

INDEX

ORDER FORM

ISARR
85 Great Portland Street
First Floor
London, W1W 7LT

Order Number:	
Agreement Date**:**	
Company:	
Address:	
Contact Email:	

Module	**Description**	**Year1**	**Year2**	**Year3**
		yr1 total	yr2 total	yr3 total
	TOTAL (Exc VAT)			
Options				
Premium Support	Optional 247 out of hours support (not currently included)	£3,000	£3,000	£3,000

Send all correspondence to:

ISARR, 85 Great Portland Street,
First Floor, London, W1W 7LT
Email : accounts@ISARR.com
Phone : 0844 736 2544

For *[Insert Company name]*	
Signature:	
By:	***[signatory name]***
Title:	***[signatory Title]***
Date:	***[Date Of Agreement]***

For ISARR	
Signature:	
By:	
Title:	
Date:	***[Date Of Agreement]***

ISARR SERVICE TERMS AND CONDITIONS

DEFINITIONS

In these Terms the following words and expressions shall, where the context so admits, have the following meanings

"Customer" the company, firm, local authority, borough council, emergency Service or other organisation named in the Order

"Agreement" the Order and these Terms

"ISARR" or "SUPPLIER" "Comunis Limited, trading as ISARR whose registered office is at 85 Great Portland Street, First Floor, London, W1W 7LT (Company Registration Number: 04823119)

"Order" ISARR Purchase Order form signed by the Client

"Service" the provision of access granted by ISARR to the Client to the Service throughout the Agreement Period and the access of Users to the Service via means of electronic communication

"Terms" these Terms of business

"Users" those persons, firm, company or other organisations identified in the Order who will have access to and use of the Service

"Data Breach" means; any breach of security, breach of the Data Privacy Laws or breach of the Supplier's obligations under this Amendment Agreement or the Existing Agreement or any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Personal Data;

"Data Controller" has the meaning given to that term (or to the term 'controller') in Data Privacy Laws;

"Data Processor" has the meaning given to that term (or to the term 'processor') in Data Privacy Laws;

"Data Privacy Laws" means all statutes, laws, secondary legislation and regulations pertaining to privacy, confidentiality and or data protection of Personal Data or corporate data, including (but not limited to) the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI2003/2426), the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)), E-Privacy Regulation, General Data Protection Regulation ((EU) 2016/679)) and any relevant national laws implementing Directives 95/46/EC, 2002/58/EC 7 97/66/EC or General Data Protection Regulation ((EU) 2016/679)) to the extent applicable to this Amendment Agreement and the relationship between the Parties;

"Data Protection Losses" means all liabilities, including all:

a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage);
b) to the extent permitted by Data Protection Law, all administrative fines, penalties, sanctions, liabilities or other remedies imposed by a supervisory authority, as well as any compensation which must be paid to a Data Subject by order of a supervisory authority.

"Data Subject" has the meaning given to that term in Data Privacy Laws;
"Data Subject Request" means a request made by any person to exercise any rights of a data subject;
"GDPR" means EU General Data Protection Regulation 2016/679;
"DPA 2018" means Data Protection Act 2018;

"Model Contractual Clauses" means the contractual clauses set out in Schedule 2, amended as indicated (in square brackets and italics) in that Schedule

"Personal Data" has the meaning given to that term in Data Privacy Laws;
"Processing" has the meaning given to that term in Data Privacy Laws (and related terms such as Process have corresponding meanings);

"Processing Instructions" has the meaning given to that term in paragraph 4.1(a);

"Supervisory Authority" means the local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Privacy Laws in the United Kingdom;

1. ABOUT ISARR

1.1 ISARR is an Application Service Provider. It provides the Customer with online security, risk and business continuity Services as specified in the Customer's Order and on the Terms set out below.

1.2 Comunis Ltd trading as ISARR, is a company registered under the laws of England and Wales. Its company registration number is 4823119 and its registered office is 85 Great Portland Street, First Floor, London, W1W 7LT.

1.3 ISARR's trading address is 85 Great Portland Street, First Floor, London, W1W 7LT . All communications with ISARR, including any complaints, should be made to this address, unless made by email to the email address given in the Contact area of our website at www.isarr.com

1.4 Enquiries relating to technical support should be made via the ISARR support ticket system within the application or via email to the ISARR technical support system; support@isarr.com

2. SERVICE SPECIFICATION

2.1 ISARR shall provide the Service in accordance with the Service description within the Customer's Order, subject to the limitations set out in this Agreement and in ISARR's Essential Operational Processings (ANNEX 1)

2.2 Service Level Guarantees are only provided where a separate 'Service Level Agreement' has been entered into and the Terms and Conditions of those Services will be documented there (ANNEX 2)

2.3 ISARR reserves the right to modify the Service description in Order to improve the quality or effectiveness of the Service without the prior consent of the Customer. ISARR will notify the Customer of any changes and these will be shown to the Customer as part of an agreed change management process, before any changes are made to the main Service

2.4 ISARR may modify its Data Protection and Privacy Policy without the further consent of the Customer so as to ensure that they comply with all relevant legislation or regulatory guidance and/or to bring them into line with common industry practice. Once a modification has taken place written notification will be sent to the Customer.

3. SERVICE CHARGES AND PAYMENT

3.1 Customer agrees to pay ISARR charges, as specified within the Service description within the Customer's Order.

3.2 The Service period will be for 3 years with a 12 month minimum term and annual break clause. All fixed costs for each annual period and all predictable additional service costs will be agreed upfront and included within the annual purchase Order

3.3 Service charges will be invoiced in advance annually. If on account Terms, payment must be received by ISARR within 45 days after the date of the invoice. ISARR may charge daily interest on outstanding amounts until payment in full is received at a rate equal to 4 per cent per annum above the Bank of England Base Lending Rate as current from time to time. If on pay in advance Terms, payment must be received by ISARR by the due date agreed and subsequently by the due date of any Service renewal.

3.4 All sums due to ISARR under any Order are exclusive of Value Added Tax ("VAT"), and any other use or sales taxes, duties, or levies imposed by any authority, government, or government agency which may apply or be introduced from time to time which shall be charged thereon in accordance with the relevant regulations in force at the time of providing the Service and shall be paid by the Customer.

4. DUTIES AND RESPONSIBILITIES

4.1 Customer agrees to pay in accordance with agreed rates defined in the customer’s order for maintenance and other Service activities relating to the Service.

4.2 The Service will be furnished to Customer subject to the condition that it will not, nor will it permit others to use the Service for unlawful purposes or any purpose for which the Service was not designed.

4.3 Customer will indemnify and save ISARR harmless from and against all loss, liability, damage and expense, including reasonable legal fees, caused by the negligent acts or omissions of the Customer or other user of Customer's Service which result in claims for damage to property and/or injury or death to persons, claims for libel, slander, invasion of privacy or infringement of copyright, or any actions brought pursuant to the provisions of the Data Protection Act, including any amendment, replacement, or re-enactment thereof for the time being in force, and invasion and/or alteration of private records or data arising from any information, data or message transmitted by Customer or its Users, and claims for infringement of patents arising from the use of apparatus and systems of the Customer in connection with the Service furnished by ISARR.

4.4 Customer shall use its reasonable endeavours to protect and keep confidential all ISARR software used by it and shall make no attempt to examine, copy, alter, "reverse engineer", decompile, discover the source code to, tamper with, or otherwise misuse such software.

4.5 Customer's right to use the Service is personal to Customer and its authorised Users. This right is non-exclusive and non-transferable. Customer is not permitted to sell, assign, sublicense or grant a security interest in or otherwise transfer any right in ISARR software. This Agreement does not grant Customer any right to any ISARR software except the limited right to use as set out in this clause.

4.6 Customer shall comply at all times with all relevant statutory and licensing obligations in connection with accessing and using the Service.

4.7 ISARR shall not be responsible for the installation of equipment necessary to provide the Service or for any cabling or connection.

4.8 ISARR will maintain the Service and provide Customer and its authorised Users of the Service such training, instructional material and other support Service as deemed appropriate at ISARR's then current prices for such support Services.

4.9 ISARR shall allow Customer to access relevant records as may be reasonably required in order to:

(a) fulfil any legally enforceable request by a Supervisory Authority or other regulator; or

(b) undertake verification that the Supplier's systems protect the integrity, operational availability, confidentiality and security of the Personal Data; and

(c) ensure the Supplier maintains complete and accurate records and information to demonstrate its compliance with its data processing obligations

4.10 Customer shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Supplier, or delay the provision of the services by the Supplier `and that, where possible, individual audits are coordinated with each party to minimise any disruption.

4.11 Subject to Customer's obligations of confidentiality, the Supplier shall provide Customer with all reasonable co-operation, access and assistance in relation to each audit.

4.12 permit where the Supplier becomes aware of a data breach or alleged breach of the Data Privacy Laws, reasonable access by Customer to all records, computer systems, or any other information howsoever held by the Supplier in respect of the Supplier's activities

4.13 Customer shall reasonably monitor the email accounts it has specified for communications from ISARR in relation to the Service.

4.14 The Customer is not precluded from pursuing damages in contract or tort against the Customer as a result of ISARR software downtime.

5. ISARR'S RIGHT TO SUSPEND THE SERVICE

5.1 ISARR reserves the right to suspend all or part of the Service provided to the Customer if it becomes aware of any actual or potential breach of these Terms and conditions by Customer or other user of the Customer's Service. ISARR will immediately notify the customer by both post and email in such an event. If the Customer fails to remedy any breach within 30 days after written notice then ISARR reserve the right to terminate this Agreement in accordance with the provisions in clause 9.4

5.2 ISARR reserves the right to suspend all or part of the Service if the provision of the Service might expose ISARR to criminal or civil liability of any kind. ISARR will immediately notify the customer by both post and email in such an event.

5.3 ISARR shall only restore the Service to full operation if, on the information provided to it in relation to the reason for the suspension of the Service, it in good faith reasonably judges that there is no risk of the restoration of the Service exposing it to criminal or civil liability of any kind.

5.4 ISARR reserves the right to suspend all or part of the Service if payment is not received in accordance with the Terms and conditions and such Service will only be resumed, and then entirely at ISARR's discretion, if all monies outstanding have been received by ISARR. Further this clause shall be without prejudice to ISARR's right to terminate in any event the Agreement in accordance with clause 9.4

5.5 During any period of suspension the Customer agrees to continue to pay and to remain liable for all charges pursuant to these Terms and conditions and the Customer's Order.

6. PRIVACY AND GENERAL DATA PROTECTION REGULATION

6.1 DATA CONTROLLER

The Customer will be the Data Controller and the Supplier will be the Data Processor when processing Personal Data in the course of the Supplier providing Services to the Customer under this Agreement.

(a) The Supplier acknowledges that the Customer shall solely be responsible for the following decisions and determinations:
(b) the purpose(s) for which and the manner in which the Personal Data will be Processed or used;
(c) what Personal Data to collect and the legal basis for doing so;
(d) which items (or content) of Personal Data to collect;
(e) which individuals to collect Personal Data about;
(f) whether to disclose the Personal Data, and if so, who to;
(g) whether subject access and other individuals' rights apply including the application of any exemptions;
(h) how long to retain the Personal Data; and
(i) whether to make non-routine amendments to the Personal Data.

6.2 PROCESSING OBLIGATIONS

The Supplier shall:

(a) Process Personal Data only:
  (i) in accordance with Customer's prior written instructions;
  (ii) for such other purposes as may be instructed by or agreed with Customer or as otherwise notified in writing from time to time; and
  (iii) in accordance with the Data Privacy Laws;
  (iv) and as set out in Schedule 1 (Details of Processing Activities) unless required to do so by Applicable Laws, in which case the Supplier shall inform Customer of that legal requirement before processing, unless legally prohibited. Schedule 1 of this Amendment Agreement, sets out the scope, nature and purpose of processing by the Supplier, the duration of the processing and the types of Personal Data and categories of Data Subject, and Customer may make reasonable amendments to Schedule 1 from time to time to meet the requirements of Article 28(3) of the DPA 2018/GDPR;

(b) ensure an effective information security programme is in place with administrative, technical and physical safeguards to protect Personal Data for all customers. This includes encrypted data transfer, secure storage and firewalls, intrusion detection and prevention, access controls and reporting, anti virus and anti malware, data loss prevention, systems monitoring, security threat analysis and preventative security patching.

(c) establish Technical and Organisational Measures in accordance with Article 28 Paragraph 3 Point c, and Article 32 DPA 2018/GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 DPA 2018/GDPR are taken into account.
  (i) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced.

(d) not otherwise modify, amend, remove or alter the contents of the Personal Data or disclose or permit the disclosure of any of the Personal Data to any third party without the prior written authorisation of Customer;

(e) maintain up to date records of its processing activities performed on behalf of Customer which shall include the categories of processing activities performed, information on cross border data transfers and a general description of security measures implemented in respect of processed data and provide a copy of such records to Customer upon request;

(f) unless otherwise required by Data Privacy Laws, the Supplier shall return or delete, at Customer's sole discretion, all Personal Data upon the termination of the processing activities carried out under this Amendment Agreement, and provide Customer with a confirmation in writing that it has done so within 21 days of the termination of the processing activities;

(g) ensure that only those personnel who need to have access to the Personal Data are granted access to such Personal Data (and only for the purposes of the performance of this Agreement) and that all of the personnel required to access the Personal Data:
  (i) are reliable, trustworthy, and have been trained in how to handle and process Personal Data; and
  (ii) have been informed of the confidential nature of the Personal Data and are subject to a duty of confidentiality; and
  (iii) comply with the obligations set out in this clause;

(h) assist Customer by implementing appropriate technical and organisational measures for the fulfilment of Customer's obligation to respond to requests from Data Subject's to exercise Data Subject rights under the Data Privacy Laws (including those laid down in Chapter III of the DPA 2018/GDPR including Data Subject's rights to access, rectify, erase or object to the processing of Personal Data) and shall notify Customer within 48 hours if it receives:
  (i) a request from a Data Subject to access that Data Subject's Personal Data;
  (ii) a request from a Data Subject to exercise any of their other rights under the Data Privacy Laws (for example the exercise of the right to rectification, or the right to erasure);
  (iii) any communication from the Information Commissioner's Office ("ICO") in relation to the Processing of Personal Data ("ICO Correspondence"); or
  (iv) a complaint from a Data Subject;

(i) notify Customer immediately (and no later than 24 hours after becoming aware) in the event that it becomes aware of any breach of the Data Privacy Laws and provide Customer without undue delay with such details as Customer reasonably requires in respect of the same;

(j) notify Customer without undue delay and in any case within 24 hours if it becomes aware of a Data Breach affecting Personal Data;

(k) provide reasonable assistance to Customer with any data privacy impact assessments, and prior consultations with Supervisory Authorities which Customer reasonably considers to be required by Article 35 or 36 of DPA 2018/GDPR or equivalent provisions of any other Data Privacy Laws, in relation to the Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Supplier;

(l) cooperate with the relevant Supervisory Authority in the performance of its obligations;

6.3 In the event that the Supplier believes that Customer's instructions are unlawful, the Supplier must immediately inform Customer.

6.4 **TRANSFERS OUTSIDE OF THE EEA**

Customer consents to the transfer of Personal Data by the Supplier to a country outside of the EEA, where Supplier complies with the following additional provisions:

(a) confirm in writing to Customer:
  (i) the Personal Data which will be transferred to and/or processed outside of the EEA;
  (ii) any subprocessors or other third parties who will be processing and/or receiving Personal Data outside of the EEA; (listed in Schedule 1)
  (iii) how the Supplier will ensure an adequate level of protection and adequate safeguards in respect of the Personal Data that will be processed in and/or transferred outside of the EEA so as to ensure the Customer's compliance with the Data Privacy Laws;

(b) Supplier enters into 'Standard Contract Clauses' (which are approved by the European Commission as offering adequate safeguards under the Data Privacy Laws (the "Model Clauses")) with Customer; and
  (i) procuring that any subprocessor or other third party who will be processing and/or receiving or accessing the Personal Data outside of the EEA either enters into:
    (a) a data processing agreement with the Supplier on terms which are equivalent to those agreed between Customer and the subprocessor relating to the relevant Personal Data transfer, and in each case which the Supplier acknowledges may include the incorporation of the Model Clauses at Schedule 2 and security and technical and organisation measures which Customer deems necessary for the purpose of protecting Personal Data.

6.5 **APPOINTMENT OF SUBPROCESSORS**

Supplier may hire other companies to provide limited services on its behalf, provided that Supplier complies with the provisions of this Amendment Agreement; and

(a) provide Customer with full details of the subprocessor (listed in Schedule 1 of this Amendment Agreement);
(b) the Supplier having duly executed an agreement with the relevant subprocessor which includes terms which are substantially the same as the terms set out in this Amendment Agreement
(c) the Supplier shall not disclose Personal Data to a third party in any circumstances other than to a subprocessor appointed in accordance with this clause 6 or as expressly authorised in advance in writing by the Customer.

6.6 **AMENDMENTS**

If Data Privacy Laws are amended or replaced by subsequent legislation or regulations or if case law pursuant to Data Privacy Laws and/or regulations enacted under it require amendments to this Amendment Agreement in the reasonable opinion of Customer then the Supplier will agree to such reasonable amendments to this Amendment Agreement and will enter into a deed of variation to effect such amendments.

6.7 **AUDIT**

Supplier shall allow Customer to access relevant records as may be reasonably required in order to:

(a) fulfil any legally enforceable request by a Supervisory Authority or other regulator; or
(b) undertake verification that the Supplier's systems protect the integrity, operational availability, confidentiality and security of the Personal Data; and

(c) ensure the Supplier maintains complete and accurate records and information to demonstrate its compliance with its data processing obligations

6.8 Customer shall use its reasonable endeavours to ensure that the conduct of each audit does not unreasonably disrupt the Supplier, or delay the provision of the services by the Supplier `and that, where possible, individual audits are coordinated with each party to minimise any disruption.

6.9 Subject to Customer's obligations of confidentiality, the Supplier shall provide Customer with all reasonable co-operation, access and assistance in relation to each audit.

6.10 permit where the Supplier becomes aware of a data breach or alleged breach of the Data Privacy Laws, reasonable access by Customer to all records, computer systems, or any other information howsoever held by the Supplier in respect of the Supplier's activities pursuant to this Amendment Agreement for the purposes of reviewing compliance with the Data Privacy Laws;

6.11 **CONSEQUENCES OF TERMINATION OF THE EXISTING AGREEMENT**

Upon termination of the Existing Agreement:-

(a) the Supplier shall, at Customer's option, either forthwith return to Customer all copies of the Personal Data which it is Processing or has Processed upon behalf of Customer, or securely destroy the same within 21 days of being requested to do so by Customer unless the Supplier is specifically required to retain the Personal Data by Data Privacy Laws or Union or Member State Laws; and;

(b) the Supplier shall cease Processing Personal Data on behalf of Customer.

6.12 **LIABILITY AND INDEMNITY**

The Supplier shall indemnify, defend and hold harmless Customer and its respective directors, officers, agents, successors and assigns from any and all Data Protection Losses arising from or in connection with:

(a) any breach by the Supplier, any sub-contractor or sub-processor and/or the Supplier Personnel of the obligations set out in this Amendment Agreement;

(b) any breach of the Data Privacy Laws caused by the Supplier's act or omission

7. WARRANTIES

7.1 ISARR's sole liability for any damages due to any defect or non-performance of the Service is limited to those actually proven as directly attributable to ISARR, subject to a ceiling of 5,000,000 pounds in any one occurrence under this Agreement.

7.2 ISARR will not be responsible for any delay in or failure of the Service due to any occurrence beyond ISARR's control.

7.3 ISARR gives no warranties and accepts no responsibility in relation to the information of third parties accessed by Customer by means of the Service.

7.4 Nothing in this Agreement shall be construed as to limit or exclude either party's liabilities in respect of death or personal injuries, or any inalienable statutory consumer rights of the Customer.

7.5 To the extent that the exclusions and limitations in this Agreement are in any jurisdiction contrary to any statute or rule of law, such exclusions and limitations are to that extent dis-applied.

8. CANCELLATION BEFORE COMMENCEMENT

8.1 Once performance of this Agreement has commenced, Customer may not cancel this Agreement (although Customer may terminate the Agreement in accordance with the Terms set out below).

8.2 Prior to ISARR commencing performance of this Agreement, Customer may cancel this Agreement by informing ISARR of its intention to cancel within 7 days of the day after it entered into this Agreement with ISARR. Customer is advised to communicate either by post or email as set out in Clause 11.1 of this Agreement.

9. TERM AND TERMINATION

9.1 Once performance has commenced, this Agreement shall continue until terminated by either Party.

9.2 Either party may terminate the Contract on the giving of 3 months' notice in writing to the other, such notice to commence at the end of the current Service Period (3 year period with annual break clause. See Service Charges & Payment, 3.2)

9.3 ISARR shall not be required to give notice of the beginning of its performance hereunder. ISARR reserves the right to disconnect the Service if Customer does not fulfil its obligations under this Agreement.

9.4 In the event of default which include failure by Customer to pay any amounts within 90 days of such payment falling due; or failure by either Party to cure any breach of a term or condition in this Agreement within a reasonable period after written notice; or if an interim Order is made, or a voluntary arrangement approved, or if a petition for a bankruptcy Order is presented, or a bankruptcy Order is made by either Party, or a voluntary arrangement is approved or an administration Order is made, or a receiver or administrative receiver is appointed of any of either Party's assets or undertaking or a resolution or petition to wind up either Party is passed or presented (otherwise than for the purposes of reconstruction or amalgamation); or if any circumstances arise which entitle the Court or a creditor to appoint a receiver, administrative receiver or administrator or to present a winding-up petition or make a winding-up Order, the other party shall be entitled to terminate this Agreement without further liability.

9.5 In the event that ISARR fails to meet the network uptime guarantee (as specified in ANNEX ‘A’) the customer has the right to immediately cancel this agreement at any point throughout the duration of the contractual period with no further financial liability beyond the cancellation date.

9.6 Upon termination of the Existing Agreement;

(a) ISARR shall, at Customer’s option, either forthwith return to Customer all copies of the Personal Data which it is Processing or has Processed upon behalf of Customer, or securely destroy the same within 21 days of being requested to do so by Customer unless ISARR is specifically required to retain the Personal Data by Data Privacy Laws or Union or Member State Laws; and

(b) ISARR shall cease Processing Personal Data on behalf of Customer.

10. GENERAL

10.1 All notices (save where otherwise provided in this Agreement or in applicable legislation) from either party to the other shall be sent by first class prepaid post or by email. ISARR shall send all notices to Customer's billing address or to the email account notified to it by Customer. Customer shall send all notices to ISARR's address or email address, as set out in Clause 1 of this Agreement.

10.2 This Agreement may not be assigned, delegated, transferred or otherwise dealt with, without the prior written consent of ISARR. Customer authorises ` to assign or transfer this Agreement, including any and all billing and Service provisioning activities, to any third party for Service to be provided outside the UK as necessary to enable ISARR to provide the Service, excluding personal data unless accessed via an authorised user whilst travelling outside of the United Kingdom.

10.3 Save as otherwise provided for in this Agreement, this Agreement may not be waived, altered, or modified, except by a document in writing signed by authorised representatives of ISARR and Customer. No agent, employee or representative of ISARR or Customer has any authority to bind ISARR or Customer to any affirmation, representation or warranty unless such is specifically included in this written Agreement.

10.4 The section headings in this Agreement are inserted for convenience only and are not intended to affect the meaning or interpretation of this Agreement

10.5 This Agreement shall be governed by and construed and interpreted in accordance with English law, and the parties submit to the jurisdiction of the English Courts.

10.6 If any provision or provisions of this Agreement shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not be in any way affected or impaired thereby.

10.7 The parties further agree that this agreement constitutes the complete and exclusive statement of the agreement between them and supersedes all proposals, oral or written and all other communications between them relating to the subject herof. This order shall cumulatively contain the entire contract between the parties.

10.8 We are continually reviewing our Terms and Conditions in line with the Services we provide to our Customers. Should you have any comments to make concerning the contents, please contact us. – support@isarr.com

SCHEDULE 1 DETAILS OF PROCESSING ACTIVITIES

This Schedule includes certain details of the Processing of Personal Data as required by Article 28(3) DPA 2018/GDPR

1. **SUBJECT MATTER**

1.1 The Customer is the Data Controller and uses Supplier's online software solution "ISARR" as a so-called Software as a Service (SaaS). The terms for the use of ISARR is regulated under this Amendment Agreement.

1.2 The Subject matter of the Contract regarding the processing of data is the execution of the following services or tasks by the Supplier as the Data Processor as follows:

(a) ISARR provides, among other things, an integrated solution for planning, tracking and status reporting of tasks and risk management criteria, through web based software solutions, including delivery of messaging and notifications through in application modules.

1.3 Customer accepts the need for Supplier to carry out 'Essential Operational Processings' (listed below) so as to meet its obligations under this Amendment Agreement and Existing Agreements (Full details of the Essential Operational Processings are contained in Annex 1 ('Essential Operational Processings')

(a) Customer Data Transfer
(b) User Onboarding (individual)
(c) User Onboarding (batch)
(d) Application Maintenance (ISARR)
(e) Application Management (Data Controller/Customer)
(f) Security Breach Investigation
(g) Subject Access Request
(h) User Offboarding (Individual)
(i) User Offboarding (batch/contract termination)

1.4 Customer created content may relate to personal data, e.g. by defining responsibilities, naming them in protocols or identifying them as creators of content etc.

2. **NATURE OF PROCESSING**

2.1 The nature of the processing will include both manual and automated activity in relation to the subject matter defined in this agreement including;

(a) Automated processing of data within the ISARR system
(b) Manual processing of data by Customer and it's agents in accordance with this agreement
(c) Manual processing of data by ISARR's employees
(d) Processing of data by approved 'Third Parties' in accordance with this agreement

2.2 The undertaking of the contractually agreed processing of personal data shall be carried out in accordance with the Contract and the Service Agreement within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA)

3. **PURPOSE OF PROCESSING**

3.1 The Supplier will process Personal Data in support of the services provided under this Amendment Agreement.

4. **SUB PROCESSORS**

Organisation	Purpose
Upcloud	Data Centre Infrastructure Hosting
Postmark	Transactional email delivery
AWS	Firewall WAF DDOS Route 53 resilient DNS
MailGun	Transactional email scalable delivery
MessageBird	Programmatic messaging – SMS and Voice
G Suite	Google email and collaboration (ISARR internal)

5. **TYPE OF PERSONAL DATA**

5.1 Personal Data including, but not limited to;

(a) names
(b) addresses
(c) date of birth
(d) contact details (including phone and email address)
(e) exchanges of letters/email
(f) contemporaneous notes reflecting verbal contacts
(g) copies of inbound and outbound correspondence
(h) copies of relevant documents and associated relevant information

6. **CATEGORIES OF DATA SUBJECTS**

6.1 Personnel whose data is processed by the Supplier for the performance of the Services including;

(a) Employees
(b) Customers
(c) Authorised Agents
(d) Contact Persons
(e) Subscribers
(f) Suppliers
(g) Other persons using or mentioned in ISARR
(h) Potential Customers
(i) Members of 'The Public' where Customer has a legal obligation to monitor and or record public spaces.

7. **SENSITIVE PERSONAL DATA**

7.1 Sensitive personal data, including Special Category data subject to a 'Data Protection Impact Assessment' (DPIA) and the establishment of a lawful basis in compliance with 'Article 9' of the DPA 2018/GDPR personal data revealing racial or ethnic origin;

(a) personal data revealing political opinions;
(b) personal data revealing religious or philosophical beliefs;
(c) personal data revealing trade union membership;
(d) genetic data;
(e) biometric data (where used for identification purposes);
(f) data concerning health;
(g) data concerning a person's sex life; and
(h) data concerning a person's sexual orientation.

8. **RECIPIENTS OF THE PERSONAL DATA**

8.1 The Supplier and its sub-processors in connection with the provision of services under this agreement.

8.2 Customer and it's authorised representatives at the express and written permission of Customer, only in accordance with this agreement, Existing Agreements and or the Service Agreement

9. **DATA TRANSFERS**

9.1 To the recipients of the Personal Data as noted above in accordance with this agreement.

9.2 Any person (natural or legal) or organisation to whom the Supplier may be required by applicable law or regulation to disclose Personal Data, including law enforcement authorities (e.g. the Information Commissioner's Office (ICO)

10. **DURATION**

11. The Personal Data will be processed in each case for the amount of time necessary for the Supplier to carry out the processing activities and following completion of such processing activities the Supplier will at the absolute discretion of Customer, return or delete all Personal Data unless otherwise required by Data Protection Laws.

SCHEDULE 2 MODEL CONTRACTUAL CLAUSES

[These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws;

(i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the DPA 2018/GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or

(ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law (otherwise).]

[If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".]

MODEL CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection [This opening recital is deleted if these Clauses are not governed by the law of a member state of the EEA.]

Name of the data exporting organisation:	*[Insert Company Name]*
Address:	*[Insert CompanyAddress]*
Email :	*[Company email]*
Phone :	*[Company phone]*
Fax:	*[Company fax]*

(the Customer)

And

Name of the data importing organisation:	**ISARR**
Address:	**85 Great Portland Street, First Floor, London, W1W 7LT**
Email :	**dpa@ISARR.com**
Phone :	**0844 736 2544**

(the Customer)

each a “party”; together “the parties”, have agreed the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Customer to the Supplier of the personal data specified in Appendix 1

BACKGROUND

The Customer has entered into a data processing addendum ("DPA") with the Supplier. Pursuant to the terms of the DPA, it is contemplated that services provided by the Supplier will involve the transfer of personal data to Supplier. Supplier or its Sub-Processors is located in a country not ensuring an adequate level of data protection under EU Adequacy decisions. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the Supplier's execution of, and compliance with, the terms of these Clauses.

CLAUSE 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; [If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data" are added.]

(b) 'the Customer' means the controller who transfers the personal data;

(c) 'the Supplier' means the processor who agrees to receive from the Customer personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; [If these Clauses are not governed by the law of a Member State, the words "and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC" are deleted.]

(d) 'the subprocessor' means any processor engaged by the Supplier or by any other subprocessor of the Supplier who agrees to receive from the Supplier or from any other subprocessor of the Supplier personal data exclusively intended for processing activities to be carried out on behalf of the Customer after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the Customer is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

CLAUSE 2

Details of the transfer
The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

CLAUSE 3

Third-party beneficiary clause
1. The data subject can enforce against the Customer this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the Supplier this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the Customer has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the Customer by contract or by operation of law, as a result of which it takes on the rights and obligations of the Customer, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the Customer and the Supplier have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the Customer by contract or by operation of law as a result of which it takes on the rights and obligations of the Customer, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

CLAUSE4

Obligations of the Customer
1. The Customer agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the Customer is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the Supplier to process the personal data transferred only on the Customer's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the Supplier will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; [If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.]

(g) to forward any notification received from the Supplier or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the Customer decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the Supplier under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

CLAUSE 5

Obligations of the Supplier

1. The Supplier agrees and warrants:

(a) to process the personal data only on behalf of the Customer and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the Customer of its inability to comply, in which case the Customer is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the Customer and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the Customer as soon as it is aware, in which case the Customer is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the Customer about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the Customer relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the Customer to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the Customer or an

inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the Customer, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the Customer;

(h) that, in the event of subprocessing, it has previously informed the Customer and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the Customer.

CLAUSE 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the Customer for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the Customer, arising out of a breach by the Supplier or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the Customer has factually disappeared or ceased to exist in law or has become insolvent, the Supplier agrees that the data subject may issue a claim against the Supplier as if it were the Customer, unless any successor entity has assumed the entire legal obligations of the Customer by contract of by operation of law, in which case the data subject can enforce its rights against such entity.
The Supplier may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the Customer or the Supplier referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the Customer and the Supplier have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the Customer or the Supplier, unless any successor entity has assumed the entire legal obligations of the Customer or Supplier by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

CLAUSE 7

Mediation and jurisdiction

1. The Supplier agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the Supplier will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the Customer is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

CLAUSE 8

Cooperation with supervisory authorities

1. The Customer agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the Supplier, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the Customer under the applicable data protection law.

3. The Supplier shall promptly inform the Customer about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the Supplier, or any subprocessor, pursuant to paragraph 2. In such a case the Customer shall be entitled to take the measures foreseen in Clause 5 (b).

CLAUSE 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the Customer is established.

CLAUSE 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

CLAUSE 11

Subprocessing

1. The Supplier shall not subcontract any of its processing operations performed on behalf of the Customer under the Clauses without the prior written consent of the Customer. Where the Supplier subcontracts its obligations under the Clauses, with the consent of the Customer, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the Supplier under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the Supplier shall remain fully liable to the Customer for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the Supplier and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the Customer or the Supplier because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the Customer or Supplier by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the Customer is established.

4. The Customer shall keep a list of subprocessing agreements concluded under the Clauses and notified by the Supplier pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Customer's data protection supervisory authority.

CLAUSE 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the Supplier and the subprocessor shall, at the choice of the Customer, return all the personal data transferred and the copies thereof to the Customer or shall destroy all the personal data and certify to the Customer that it has done so, unless legislation imposed upon the Supplier prevents it from returning or destroying all or part of the personal data transferred. In that case, the Supplier warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The Supplier and the subprocessor warrant that upon request of the Customer and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the Customer:

Name (written out in full):	*[signatory name]*
Position:	*[SignatoryTitle]*
Company Address:	*[CompanyAddress]*

Signature: On behalf of the Customer	*[Customer signature here]*

On behalf of the Supplier:

Name:	**Nick Beale**
Position:	**Managing Director**
Address:	**ISARR** **85 Great Portland Street** **First Floor** **London, W1W 7LT**

Signature: On behalf of the Supplier	

APPENDIX 1 TO THE MODEL CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Customer

The Customer is:
[Insert Company Name]

Supplier

The Supplier is:
ISARR LIMITED

Data subjects
As set out in the Amendment Agreement and as required for the supplier to provide services to the customer.

Categories of data
Personnel whose data is processed by the supplier for the performance of the services.

Special categories of data (if appropriate)
Information relating to health, political opinions, race or ethnicity, religious beliefs, trade union membership, genetic or biometric information, sex life or sexual orientation, or criminal convictions or offences.

Processing operations
The supplier will process personal data in support of the services provided under this Amendment Agreement.

Customer:

Signature: On behalf of the Customer	*[Customer signature here]*

Supplier:

Signature: On behalf of the Supplier	

APPENDIX 2 TO THE MODEL CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed by the Supplier.

Description of the Technical and Organisational Security Measures implemented by the Supplier in accordance with Clauses 4(d) and 5(c):

The technical and organisational security measures implemented by the data importer are as described in and will be implemented in accordance with the terms of a master agreement currently in effect between the data exporter and the data importer or if one does not exist, by the ISARR Cloud Environment Service Guide, Technical Support Policy and Procedures, and/or the Terms and Conditions listed in any existing contract between the Supplier and the Customer.

In addition, below are generally ISARR's current technical and organizational security measures to protect the confidentiality, integrity and availability of personal data with ISARR's products and services. ISARR may change these measures at any time without notice so long as it maintains a comparable or better level of security.

- Pseudonymisation and encryption of personal data:
    - Encryption of personal data at rest: ISARR requires that personal data is encrypted at rest. This can be achieved through application level encryption, filesystem encryption or hardware based encryption at a storage media level.
    - Encryption of personal data in transit: ISARR requires that personal data is encrypted during transit by leveraging common industry protocols as Transport Layer Security (TLS) or Virtual Private Networks (VPN).

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services:
    - Access Control:
        - ISARR has implemented physical access controls at all of our offices, requiring employees and onsite-contractors to authenticate before entering the premises or special sections in the office. Third party hosting providers are required to provide evidence that physical access control requirements are met.
        - ISARR has implemented system access control for all systems that are not for public access. Access control includes the usage of a username and a complex password and, with critical systems, multifactor authentication leveraging one-time credentials.
        - ISARR has implemented network access control at all the ingress and egress network points. All network traffic is denied by default. Only traffic that meets an access control rule is allowed into the corporate network.
    - Awareness and Training:
        - ISARR requires all new employees to take general security & privacy awareness training and employees and contractors are required to complete the security & privacy awareness training on an annual basis. This includes passing an exam demonstrating the knowledge the training conveys.
        - ISARR requires job-specific security & privacy training for employees and agents in security & privacy critical roles, providing additional security & privacy knowledge and skills.
    - Logging & Monitoring:
        - Critical log events have been identified for all critical systems. These critical log events include information that is meaningful in identifying security incidents
        - ISARR has installed file integrity monitoring on critical systems. Any unauthorized change of files monitored would be detected and investigated.
        - Logs for critical systems are maintained according to the retention time required by law, regulation, business need or standard best practice.

- Configuration Management
  - ISARR has established secure baseline configuration for its critical systems. Baselines are reviewed and updated as new security threats or needs are identified.
  - ISARR has established Change Management processes for its critical systems. Every change request must be reviewed for impact, back-out procedure and approved by the Change Management Approval Group (CMAG)
- Identification and Authentication:
  - ISARR has established Identification and Authentication Policy and Procedures for its critical systems.
- Maintenance:
  - ISARR has implemented processes that allow for controlled maintenance of its critical systems by third party vendors.
- Media Protection:
  - ISARR has established Digital Media Handling Procedures addressing media access, media marking, media storage, media transport and media sanitisation.
- Physical and Environmental Protection:
  - ISARR requires that its data center hosting providers meet at a minimum SOC-2 and ISO27001 requirements. Hosting providers that host systems storing or processing regulated customer data (e.g., Protected Health Information (PHI) or card holder data) are required to have additional attestations in place, ensuring compliance and alignment with laws, regulations and business needs.
  - ISARR uses Public Cloud service providers, e.g Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, as Sub-Processors providing the Hosted Service. The Public Cloud service providers meet SOC-2, ISO27001, HIPAA and PCI-DSS requirements.
  - Each year ISARR requests the Public Cloud service providers to provide updated documentation that demonstrate their compliance with those security standards/frameworks.
  - ISARR ensures that it has DPA's in place with third party providers that are not located within a jurisdiction that falls under EU Adequacy decisions
- Personnel Security:
  - ISARR screens employees as well as contractors, including with a financial and a criminal background check, before providing initial access to any corporate systems.
  - ISARR revokes all access of employees upon termination.
  - ISARR adjusts access rights of personnel whenever they are transferred or assume different responsibilities within the organisation

    - System and Services Acquisitions:
        - ISARR has established acquisition processes that incorporate security into the evaluation of a vendor as well as ensuring the confidentiality, integrity and availability of its data.
    - System and Communications Protection:
        - Hardening of systems is part of the deployment of new critical systems.
        - Encrypted communication is used for all sensitive communication between systems.
    - System and Information Integrity:
        - Flaw remediation (patching) is conducted on a regular basis with systems or when deemed critical, e.g. zero-day exploits.
        - File integrity monitoring is used to ensure that critical systems are protected from unauthorized changes by users or malicious code.
    - Program Management:
        - ISARR has defined a system development lifecycle that addresses security. It establishes “security gates” with projects, ensuring that requirements and design address potential security threats
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident:
    - ISARR has taken steps to ensure it’s business continues to operate, even during a disaster disrupting normal mode of operation. Critical systems and services have been identified and regular exercises are being held to ensure that personnel are prepared in the event that disaster recovery procedures must be invoked.
    - Backups are completed nightly, ensuring that critical systems can be restored with minimal data loss.
    - ISARR has established incident response procedures, allowing for handling of incidents in a timely and controlled manner and in accordance with applicable law and obligations.
    - ISARR has defined contingency plan(s) for its critical systems. Those plan(s) are tested at least annually and updated as needed.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing:
    - Independent third-party audits/certifications:
        - IASME Gold
        - Cyber Essentials
    - Vulnerability Scans
        - ISARR has established weekly internal scans of its systems, identifying security vulnerabilities that need to be addressed.
        - Annual external scans
    - Independent third-party pen-test: Semi-annual pen-tests
    - Internal Security Assessments
        - ISARR performs an annual audit of its Information Assurance Framework
    - Risk Assessment:
      ISARR conducts annual, quarterly and monthly Risk Assessments of its key Risks with all actions recorded in the Risk register.

ANNEX 1 ESSENTIAL OPERATIONAL PROCESSINGS

INTRODUCTION

In order for ISARR to deliver the 'Application' to the customer, in accordance with any contract agreement between ISARR and the customer, and remaining fully compliant with all relevant regulations including DPA 2018/GDPR, the customer must address and make provision for the following; understanding that the ability of ISARR to deliver the product will depend on any limitations resulting from;

- The customers perception of the Data Controller/Data Processor relationship and corresponding limitations imposed by the customer
- 'Joint Controller' status with third party users not directly under the control of the customer
- DPA 2018/GDPR constraints on ISARR regarding;
    - Data retention
    - Data access
    - Liability
- Acceptance of ISARR Application 'Essential Operational Processings'

THE CUSTOMER AS DATA CONTROLLER

It is the responsibility of the customer to understand its role as Data Controller in accordance with DPA 2018/GDPR and ensure that the customer is in compliance with all aspects of DPA 2018/GDPR. ISARR will meet its obligations as Data Processor.

Consideration must be given to the balance of limitations the customer places on ISARR against ISARR's ability to deliver the 'Application' effectively. Where ISARR feels that a restriction or limitation may have an effect on delivery, ISARR will provide an alternative process that remains compliant with DPA 2018/GDPR or require the customer to agree on the reduced capability of the ISARR system in response to the process requirement.

DPA 2018/GDPR COMPLIANCE AND ASSOCIATED CONSTRAINTS

ISARR has a duty under DPA 2018/GDPR to respond to requests for information regarding data breaches and other security issues. It is perfectly possible that these requests could be made after a contract with the customer has been terminated. To this end ISARR must keep a record of the actions it took throughout the lifetime of the contract with the customer and must also keep a record of the data subjects that were held in the application including data added and dates of relevant actions.

All data retained after contract termination will be encrypted and held in secure storage on a locked down server that has restricted access via the ISARR internal VPN only.

The period for Data Retention should be set out specifically in any contract between the customer and ISARR. The Data Retention period will apply to Personal Data removed during the contract, or all data removed as a result of contract termination.

DATA ACCESS

ISARR must have continual daily access to the personal data of its customers in managing the application. This includes data migration and other server related activities, monitoring user logs, for bugs and other system issues, amongst other processes. Together these processings are bundled together as a processing group we call 'Application Maintenance'

It is not reasonably practicable for ISARR to inform the customer of each and every occasion that ISARR team members will be accessing the data. The customer must agree that for ISARR to perform its role of service provider as well as that of Data Processor, ISARR's team members will have to access Personal Data.

ISARR will ensure that its agents are correctly trained and sufficiently aware of their responsibilities in handling data in compliance with DPA 2018/GDPR (ISARR hold IASME GOLD and Cyber Essentials PLUS, 3rd Party accreditation as supporting evidence of our internal controls)

LIABILITY

ISARR must accept liability for data breaches and other failures in accordance with DPA 2018/GDPR, however, there will be occasions where the data controller/customer must accept the risk of data being accessed by system users on customer premises where ISARR has no control over the environment or actions of application users. In such circumstances ISARR cannot be liable for nefarious actions carried out by system users acting with criminal intent.

ISARR can only be liable for data accuracy where it has received data from the customer and has entered that data itself into the system inaccurately. Where the customer sends ISARR inaccurate data or enters data into the system directly, the customer must assume liability for data accuracy. To that end ISARR records all requests for data addition deletion and amendments in the 'ISARR Data Management Log'

ISARR ESSENTIAL OPERATIONAL PROCESSINGS

In order for ISARR to deliver the 'Application' effectively in accordance with the contract between ISARR and the customer, ISARR must carry out a number of 'Essential Operational Processings'. ISARR bundles together sets of 'operations' to establish a single 'Operational Processing' in accordance with Chapter 1 Article 4 'Definitions' (2) 'processing' which states:

(2) 'processing' 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;

Provision should be made by the customer, where the customer deems it necessary, to comply with DPA 2018/GDPR as 'Data Controller ' as the result of any perceived risk resulting from 'ISARR Essential Operational Processings' set out below:

- Data Transfer
- User Onboarding (individual)
- User Onboarding (batch upload)
- Application Maintenance (ISARR)
- Application Management (Data Controller/Customer)
- Security Breach Investigation
- Subject Access Request
- User Offboarding (individual)
- User Offboarding (batch)

This may mean that the customer decides to carry out a 'Data Protection Impact Assessment' (DPIA). ISARR will provide all necessary information on data processing carried out by ISARR to assist in any DPIA the customer decides to undertake.

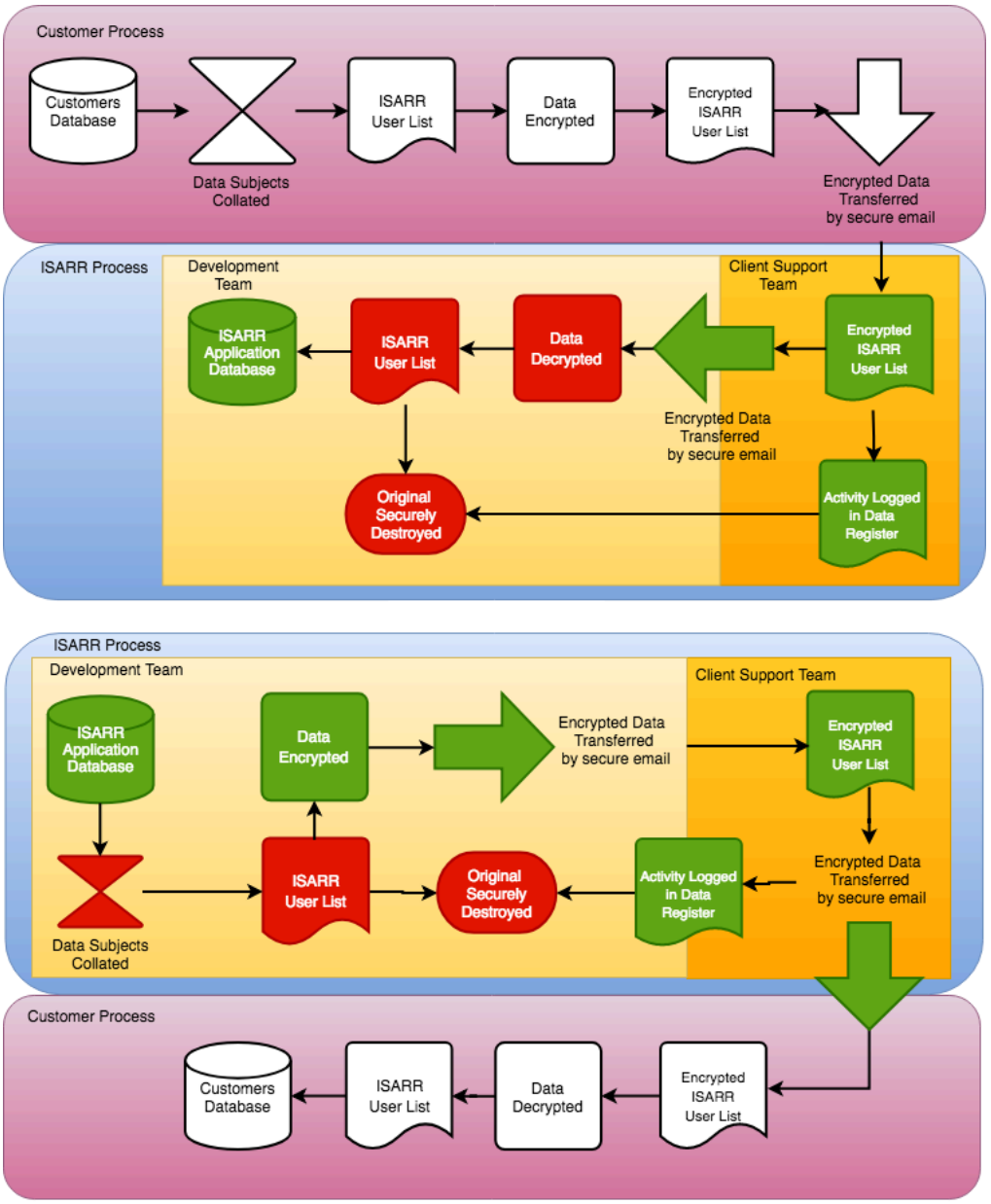
Where the customer determines a specific 'Data Processing' to be unnecessary or undesirable, ISARR will attempt to provide an alternative process, however where no such alternative is available or reasonably practicable, the customer must either accept the associated risk or accept the reduced function associated with the loss of that process.

In the process flowcharts below ISARR have identified the actions with most risk using RED icons and those actions considered less risk with GREEN icons.

1. DATA TRANSFER

There will be a number of occasions where personal data is required to be moved between the customer and ISARR, these include but are not limited to;

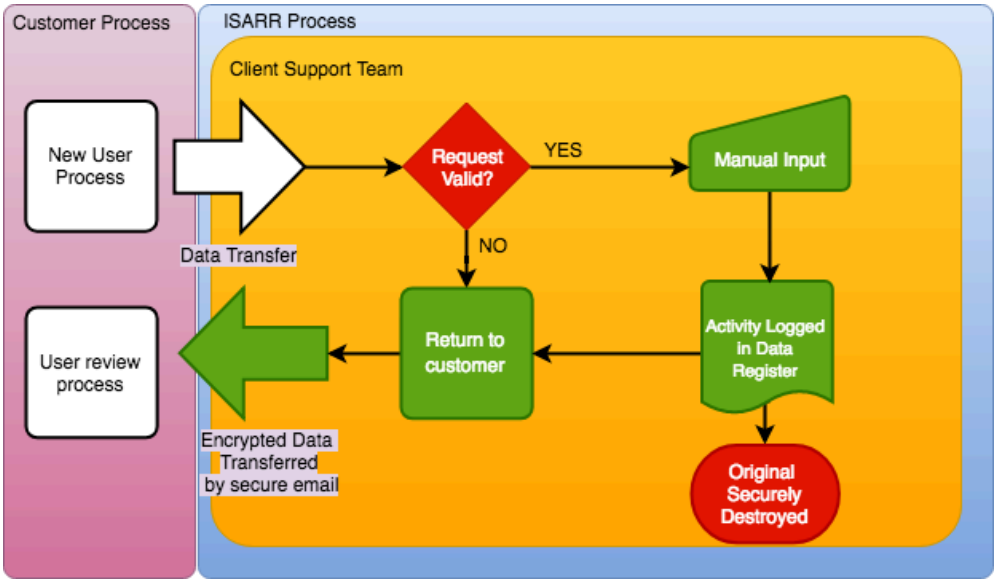
1. User Onboarding (application set up)
2. Database management
    a. Adding users
    b. Deleting users
    c. Data accuracy assessments
    d. Subject Access Request
3. User Offboarding (contract termination)



There must be an agreement between ISARR and the customer prior to any individual Data Transfer taking place. Data cannot be transferred without prior warning and agreement.

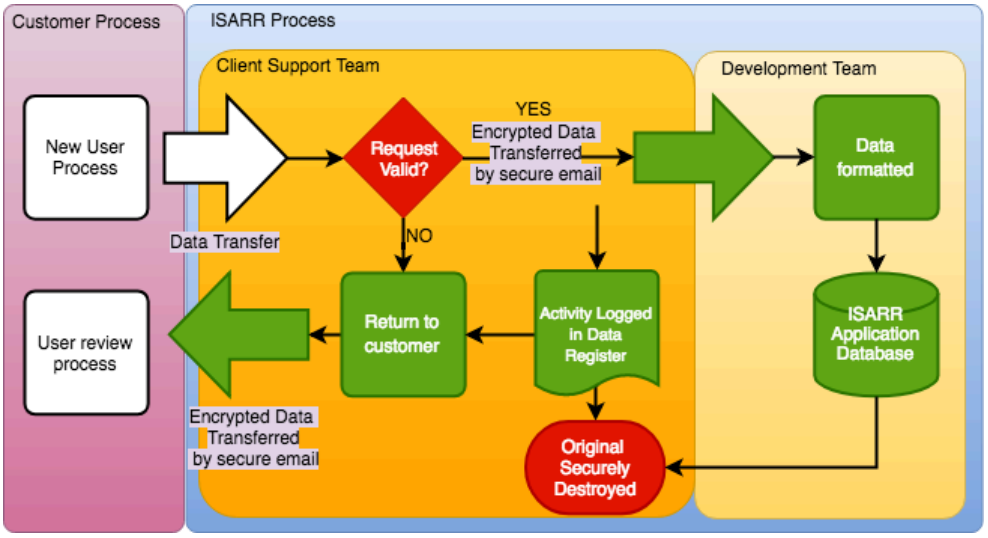
2. USER ONBOARDING (INDIVIDUAL)

Throughout the lifecycle of the contract between ISARR and the customer there will be occasion to add new users to the Application. Where the customer requires ISARR to carry out this action the process for adding individual users is as follows;



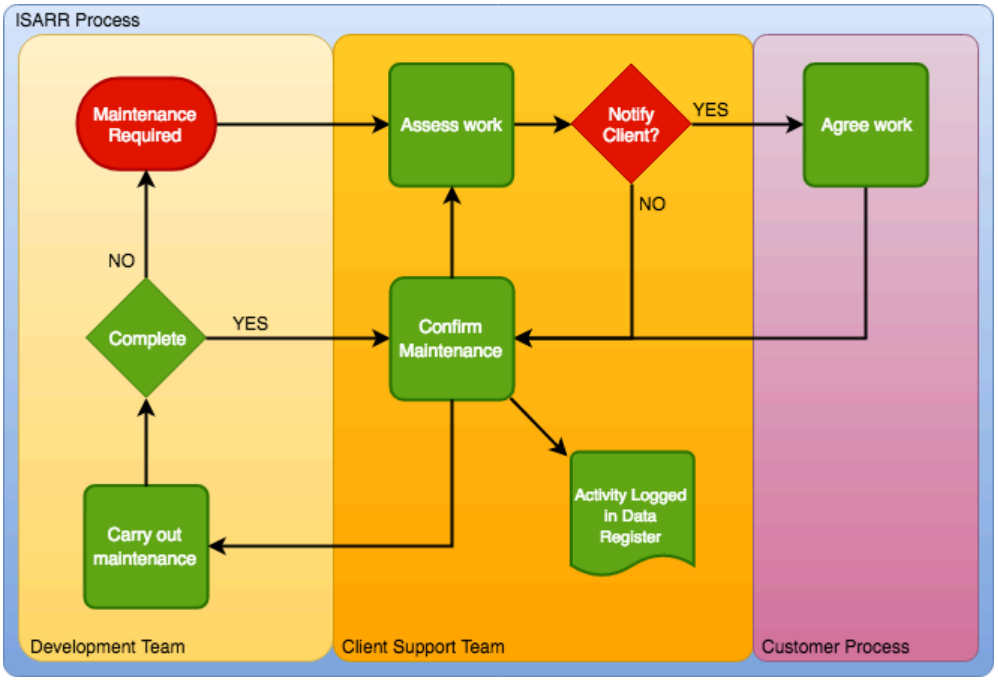
3. USER ONBOARDING (BATCH)

Where a large number of users are added to the system at the same time the onboarding process is handled via a batch upload function using csv files. This can require an extra step in formatting the original data sheet and is handled by the Development Team



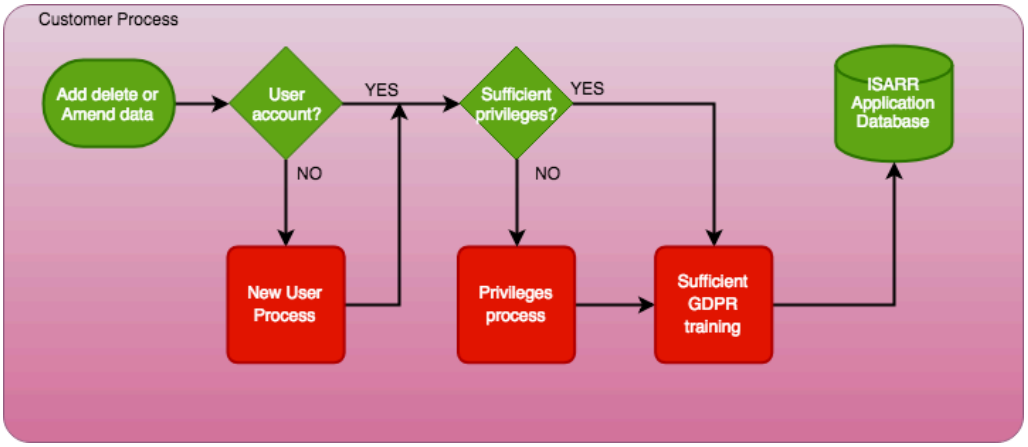
4. APPLICATION MAINTENANCE (ISARR)

Throughout the lifecycle of the contract there is an ongoing requirement for ISARR to carry out routine maintenance of the system which will inevitably include access to personal data. All such maintenance is assessed by the Client Support Team and where necessary the Client will be notified and the maintenance risk assessed and agreed.



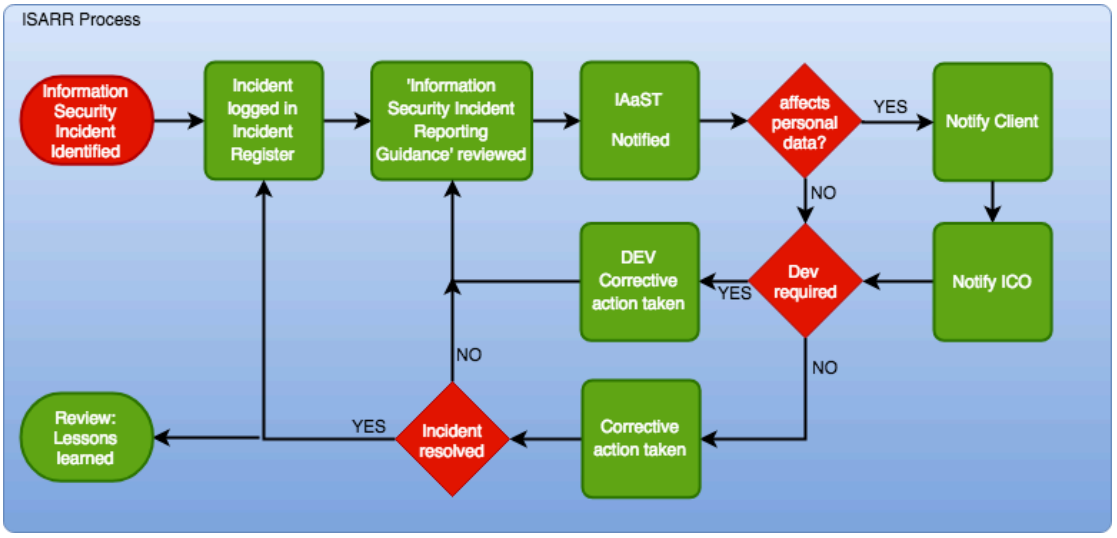
5. APPLICATION MANAGEMENT (DATA CONTROLLER/CUSTOMER)

Application management is the routine use of the ISARR application by system users. This includes standard and admin user access where the interface is through username and password in the normal fashion. Some system users will have access to personal data based on their system privileges; in such cases it must be the responsibility of the customer to ensure that its users are aware of their responsibilities for data management and handling in accordance with DPA 2018/GDPR.



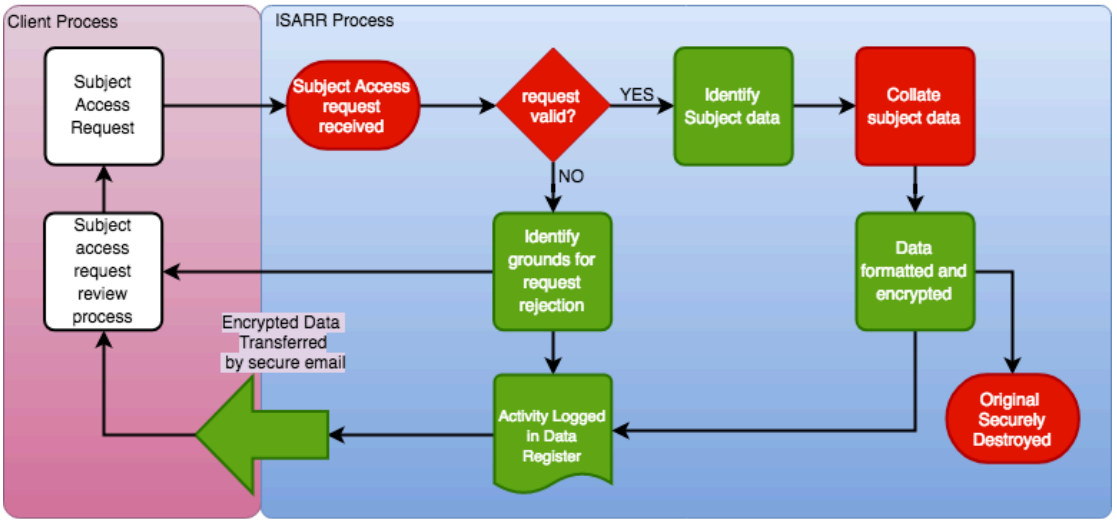
6. SECURITY BREACH INVESTIGATION

Where a Security Breach is identified, ISARR will need to access all data including personal data to review the incident severity and assess the correct course of action. In all circumstances where a breach of 'Personal Data' is identified ISARR will notify both the client and the ICO within 24 hours of the discovery.



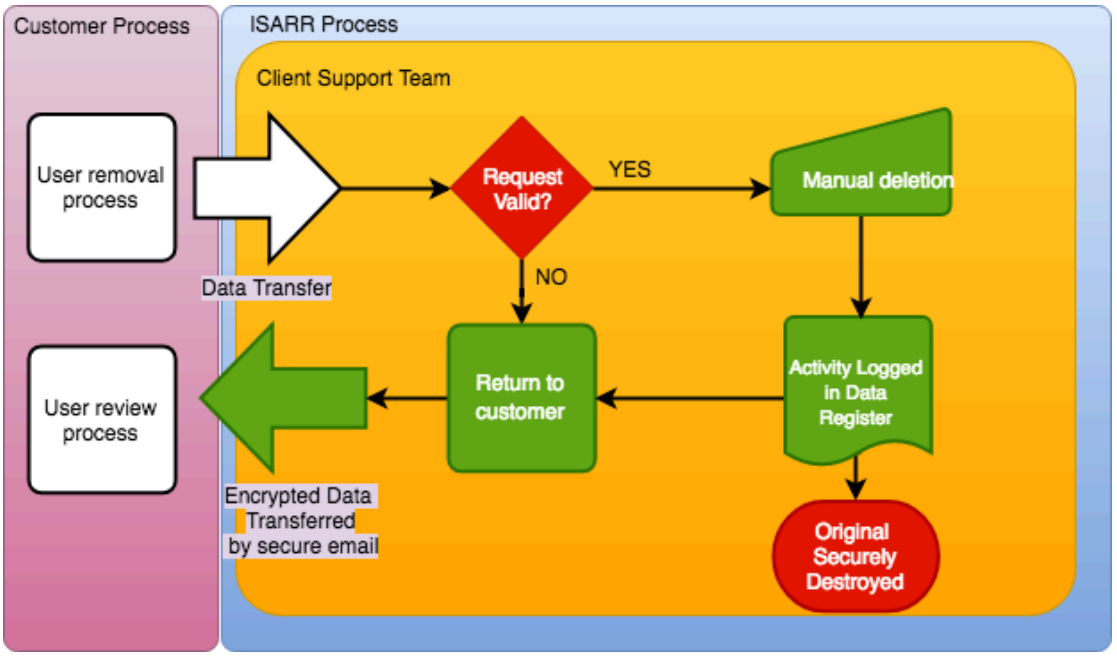
7. SUBJECT ACCESS REQUEST

DPA 2018/GDPR states that all Data Subjects have the right to know what personal information is stored related to that individual. ISARR will only process Subject Access Requests received from the Data Controller.



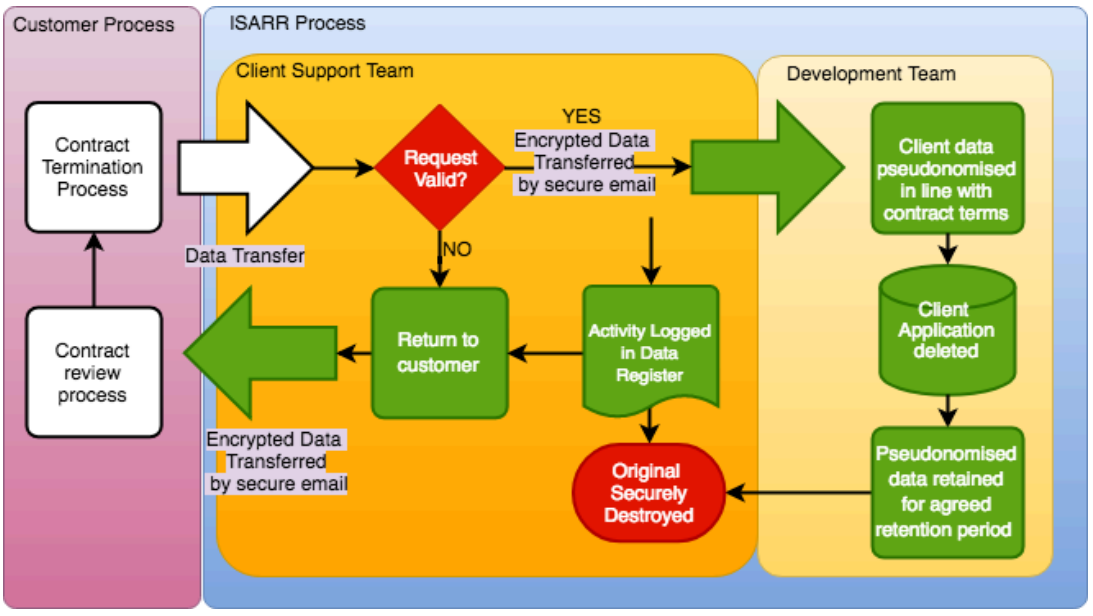
8. USER OFFBOARDING (INDIVIDUAL)

It is vital that there is a periodic review of users in the ISARR Application and that where users are no longer required to have access to, or receive notifications from the ISARR system that Data Controllers inform the ISARR team so that those users can have their data removed from the system. Failure to do so will mean that group notifications will continue to be sent to those users even after employment termination, where they receive notifications through text messages on personal devices such as mobile phones.



9. USER OFFBOARDING (BATCH/CONTRACT TERMINATION)

At the end of the contract period ISARR will, in line with the Contract, Terms and Conditions or any other existing agreements, retain application data for an agreed period to allow for data enquiries or complaints that might be submitted after the termination of any contract. Once the client agrees that all ongoing enquiries are resolved all system data will be passed to the client and deleted from ISARR servers.



10. PROCESSING RISKS

All Processings carry some risk, by definition it is impossible to have zero risk. ISARR recognises the risks associated with our processings and seeks to mitigate those risks with best practice design of systems and processes including training of staff and frequent auditing, to ensure that where we identify risks we proactively seek to reduce them to as low as is reasonably practicable.

Whenever we consider new processes internally or consider development modifications we first consider the risk that those new activities will present. ISARR operates a robust risk assessment process for both its development team and management systems and this risk assessment process forms part of our submission to The IASME Consortium when being audited for our IASME Gold standard which we are proud to have achieved.

ANNEXE 2 SERVICE LEVEL AGREEMENT AND SUPPORT CONTRACT

99.95% NETWORK UPTIME GUARANTEE

1. COVERAGE

This *Service Level Agreement* will apply to the following modules;

<based on final scope>

2. EXCLUSIONS

This SLA does not cover the following;
Short Message Service (Text/SMS) as this is reliant on the mobile carrier networks
The SLA is only valid after formal Agreement and contract to deliver Services and fees for the Service have been paid by the due date shown on the invoice for the Services

3. SERVER AVAILABILITY SERVICE LEVEL

Server Availability is the combination of both Network Availability and Critical Infrastructure Availability each defined below:

a. Network Availability

ISARR endeavours to have our Servers responding to network pings and for remote access (either by SSH, Terminal Services or other means) **99.95% of the time excluding scheduled maintenance.** Network availability is defined as ISARR's routers, switching and cabling but does not include the network card, Services or software running on the servers
Network downtime exists when a Customer is unable to access the Server and such failure is notified to ISARR by our support ticket system at support@isarr.com

Network downtime is measured from the time the support ticket is lodged to when the Server is able to respond to remote access requests.

b. Critical Infrastructure Availability

ISARR endeavours to have our Servers supplied with cool air and constant power 100% of the time excluding scheduled maintenance. Critical Infrastructure includes correct operation, all air conditioning, UPS, generator, PDU and cabling systems but excludes the server's internal power supply.

Critical Infrastructure downtime exists when a Customer is unable to access the Server and such failure is notified to ISARR by our support ticket system at support@isarr.com

Critical Infrastructure downtime is measured from the time the support ticket is lodged to when the Server is able to respond to local console access.

SOFTWARE SUPPORT CONTRACT

This Software Service Level Agreement (SSLA) identifies what the Customer can expect from ISARR. It specifies the services and commitments of ISARR and the expectations and obligations of the Customer.

1. SERVICE LEVELS

1.1 STANDARD SUPPORT

The standard support will be provided to the Customer for the duration of the contract with *ISARR*. Under the standard support service level the Customer has access to:

- General "In App" support and e-mail ticket support : support@isarr.com
- Phone support during business hours 0900 – 1730 GMT
- PDF manual on application usage, tutorials and FAQs

1.2 RESPONSE CATEGORIES

Issues will be prioritised based on Priority One, Standard Priority or Account Priority categories as detailed below;

Priority One

a. Unavailability of the network or critical infrastructure
b. Unavailability of the host server
c. Unavailability of application key module, feature or function

Standard Priority

d. Unavailability of a noncritical feature or function

Account Management

e. Noncritical user support queries

1.3 PRIORITY ONE - Response & Escalation Process

The response and escalation process for Priority One categories is detailed below;

- **First 15 mins** from receiving the support ticket request - ISARR support team will conduct basic diagnostics to attempt to identify and resolve the issue
- If the problem cannot be resolved, then it will be escalated to the Engineering Team within **30 min**. ISARR Engineers (and Data Centre Engineers if required) will work towards a resolution **within 120 minutes** from the time the ticket was escalated to the Engineering team - **Total 165** mins (**2.75 hrs**)
- Once a Priority One issue has been fixed, *ISARR* will notify the Customer administrator account holders and the user who reported the fault that the fault is resolved, and the system is fully operational. This will be done by email to the email address that is listed on the *ISARR* system.

1.4 STANDARD PRIORITY - Response & Escalation Process

The response and escalation process for Standard Priority categories is detailed below;

- **First 30 mins** from receiving the support ticket request - ISARR support team will conduct basic diagnostics to attempt to identify and resolve the issue
- If the problem cannot be resolved, then it will be escalated to the Engineering Team **within 30min**

- ISARR Engineers (and Data Centre Engineers if required) will work towards a resolution within 1 business day from the time the ticket was escalated to the Engineering team
- Once a Standard Priority issue has been fixed ISARR will notify the Customer administrator account holders and the user who reported the fault that the fault is resolved. This will be done by email to the email address that is listed on the ISARR system.

1.5 ACCOUNT MANAGEMENT - Response & Escalation Process

The response and escalation process for standard account management is detailed below;

- Support ticket received before 1300hrs on a business day will see a response within 4 hours
- Support ticket received after 1300hrs on a business day will see a response no later than 1200hrs on the next business day
- Once an Account Management support request has been resolved, ISARR will notify the Customer administrator account holders and the user who requested the support. This will be done by email to the email address that is listed on the ISARR system.

2. 24/7 OUT OF HOURS SUPPORT

2.1 24/7 Support Extension

24/7 support can be provided to the *Customer* and the **details will be covered under the project scope as required**. If the Customer has access to 24/7 support this will be provided to the Customer for the duration of the contract with *ISARR*. 24/7 support is provided for Priority One issues only, based on the response and escalation process section 3.

2.2 24/7 Support Contact

In addition to the Standard software support provided, Customer has access to:

- Dedicated phone line manned 24/7, 365 days a year

3. Support Categories, Escalation & Resolution

Issue, Escalation and Resolution Summary Table

Issue	Escalation & Resolution
Priority One	
a. Unavailability of the network or critical infrastructure	• Initial Response within 15 minutes • Resolution within 165 minutes
b. Unavailability of the Host Server	• Initial Response within 15 minutes • Resolution within 120 minutes
c. Unavailability of application key module, feature or function	• Initial Response within 15 minutes • Resolution within 180 minutes
Standard Priority	
d. Unavailability of a noncritical feature or function	• Initial Response within 30 minutes • Resolution within 1 business day
Account Management	

e. Noncritical user support queries	- Ticket received before 1300hrs on a business day will see a response within 4 hours - Ticket received after 1300hrs on a business day will see a response no later than 1200hrs on the next business day

4. Responsibilities of Those Making a Request

4.1 Whenever possible, callers should contact the Help Desk while in front of the affected equipment. Callers may be asked to provide the following information when making a request.

1. Confirm that there is no problem with local network, systems or connectivity
2. Full URL. The URL will be found in the address bar at the top of the webpage
3. User Log on details
4. Full description of problem(s)
5. Full description of error message(s)

5. SLA Performance Review

5.1 The Service Level performance will be reviewed as part of the quarterly account management review or as required, based on events.

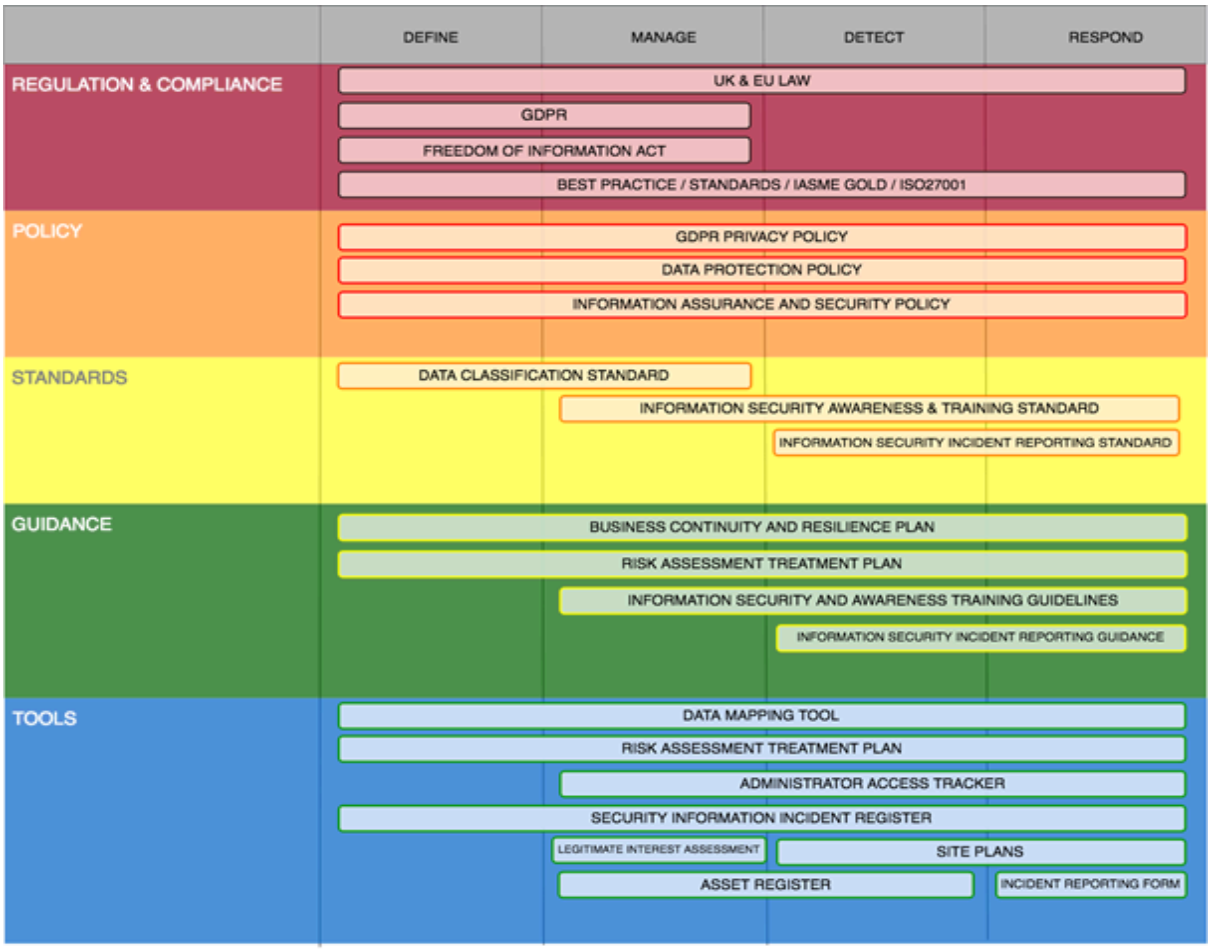
5.2 Any breach of the SLA escalation and response targets raised by the client will be reviewed and a mutual resolution/remediation plan agreed.

ANNEXE 3 ISARR DATA SECURITY AND COMPLIANCE

Data security is of the upmost importance for ISARR and its Customers. To ensure compliance with current data protection legislation, and data security best practice, ISARR have implemented and follow a comprehensive data security controls, policy and standards framework.

ISARR have been independently audited and have achieved Cyber Essentials PLUS and IASME GOLD certifications (certificate copies can be provided upon request)

As part of the certification, ISARR have implemented and follow a comprehensive Data Security, Policy, Standards and Guidance Framework



ANNEX 4 – AI MODEL TRAINING DATA OPT-IN AGREEMENT

This AI Model Training Data Opt-In Agreement (hereinafter referred to as the “AI Annex”) is an addendum to and forms part of the ISARR SERVICE TERMS AND CONDITIONS (the “Main Agreement”) entered into between:

Comunis Limited, trading as ISARR whose registered office is at 85 Great Portland Street, First Floor, **London, W1W 7LT (Company Registration Number: 04823119) ("ISARR", "SUPPLIER")**
And

[Insert Company Name] (the "Customer")

This AI Annex shall be effective from the date of acceptance by the Customer as indicated below.

WHEREAS:
A. ISARR is developing and refining an artificial intelligence model (the "AI Model") designed to analyse incident data to identify trends, patterns, and insights that may enhance the Service and provide broader benefits to its customers. B. The Customer wishes to contribute certain Anonymized Data (as defined below) to a central data pool for the purpose of training and improving the AI Model, on an optional, opt-in basis. C. This AI Annex sets out the terms and conditions under which the Customer agrees to allow ISARR to use such Anonymized Data.

IT IS AGREED AS FOLLOWS:
1. DEFINITIONS
1.1 Unless otherwise defined herein, capitalized terms shall have the meaning ascribed to them in the Main Agreement. 1.2 For the purpose of this AI Annex, the following definitions shall apply: a. **"AI Model"** means the artificial intelligence and machine learning algorithms, models, and systems developed or utilized by ISARR for the purposes described herein. b. **"Anonymized Data"** means a subset of the Customer's incident record data from which all Personal Data (as defined in the Main Agreement) has been removed and which has been processed using generalization and other modern anonymization techniques such that individual data subjects cannot be identified, directly or indirectly. Specifically, Anonymized Data shall solely consist of: i. Report Category (e.g., security breach, system failure, health and safety event); ii. Date and Time of the incident; and iii. Generalized Location Data. c. **"Generalized Location Data"** means precise geographic coordinates that have been processed using techniques (such as, but not limited to, geohashing to a lower resolution, aggregation to a broader administrative area, or introduction of controlled noise) to reduce granularity and prevent the identification or re-identification of a specific address or micro-location, while still providing useful spatial information for trend analysis. d. **"Training Data Pool"** means the aggregated collection of Anonymized Data from various ISARR customers who have opted-in under terms similar to this AI Annex, used for the training and improvement of the AI Model.

2. OPT-IN CONSENT TO USE ANONYMIZED DATA
2.1 By executing this AI Annex, or by an affirmative opt-in selection through a mechanism provided by ISARR, the Customer explicitly consents and agrees to allow ISARR to: a. Collect the specific data elements defined as Anonymized Data from the Customer’s incident records within the Service. b. Apply generalization and anonymization techniques to such data to create the Anonymized Data, ensuring the removal and protection of any Personal Data. c. Incorporate the resulting Anonymized Data into the Training Data Pool. d. Use the Anonymized Data within the Training Data Pool for the sole purpose of training, developing, maintaining, and improving the AI Model.

3. SCOPE AND PURPOSE OF DATA USAGE
3.1 ISARR warrants that it will only use the Anonymized Data for the purposes of: a. Training and refining the AI Model to improve its accuracy, predictive capabilities, and overall utility. b. Identifying systemic trends, patterns, risks, and insights from the aggregated Training Data Pool. c. Enhancing the features, functionality, and effectiveness of the Service for the benefit of its customers, including those who opt-in to data sharing. 3.2 ISARR shall not use the Anonymized Data for any purpose not

explicitly stated in this AI Annex without obtaining prior written consent from the Customer. 3.3 For the avoidance of doubt, no Personal Data, confidential information of the Customer (other than the specific elements comprising the Anonymized Data), or any data that could reasonably be used to identify the Customer specifically (beyond its contribution to an aggregated dataset) will be used for the AI Model training or shared with other customers, except as an aggregated and de-identified part of the insights generated by the AI Model.

4. DATA ANONYMIZATION AND SECURITY

4.1 ISARR commits to employing modern and robust anonymization and generalization techniques to create the Anonymized Data, consistent with applicable Data Privacy Laws (including the UK GDPR and DPA 2018) and industry best practices, with the objective of minimizing any risk of re-identification. 4.2 ISARR will maintain the security and confidentiality of the Anonymized Data in accordance with its obligations regarding data security as outlined in the Main Agreement (including but not limited to ANNEXE 3 ISARR DATA SECURITY AND COMPLIANCE). 4.3 The Customer acknowledges that while ISARR will use best efforts and modern techniques for anonymization, no anonymization technique can guarantee 100% impossibility of re-identification in all future hypothetical scenarios. However, ISARR's commitment is to ensure that the data is processed in such a manner that the personal data are no longer attributed to a specific data subject.

5. CUSTOMER ACKNOWLEDGEMENTS

5.1 The Customer acknowledges and agrees that: a. The contribution of Anonymized Data is voluntary and based on an opt-in decision. b. The Anonymized Data will be pooled with similar data from other ISARR customers. c. The insights and improvements generated by the AI Model from the Training Data Pool may be made available to other ISARR customers who participate in this data sharing initiative, and potentially as part of general service improvements. d. ISARR makes no representation or warranty that the AI Model will provide any specific benefit or outcome to the Customer.

6. NO PERSONAL DATA TRANSFER FOR AI MODEL TRAINING

6.1 It is explicitly understood and agreed by both Parties that no Personal Data will be extracted, transferred, or processed for the purpose of training the AI Model under this AI Annex. The process involves creating Anonymized Data from incident records before such data is included in the Training Data Pool. 6.2 The Customer remains the Data Controller for its Personal Data processed within the Service as per the terms of the Main Agreement. ISARR’s processing of Personal Data to create Anonymized Data shall be considered part of its role as a Data Processor, acting upon the instruction of the Customer by virtue of this opt-in AI Annex.

7. REVOCATION OF CONSENT (OPT-OUT)

7.1 The Customer may revoke its consent and opt-out of contributing further Anonymized Data to the Training Data Pool at any time by providing thirty (30) days written notice to ISARR at the address specified in Clause 11.1 of the Main Agreement or via email to accounts@ISARR.com. 7.2 Upon such revocation: a. ISARR will cease collecting and processing the Customer's data for inclusion in the Training Data Pool from the effective date of the revocation. b. Anonymized Data from the Customer that has already been incorporated into the Training Data Pool and used to train the AI Model prior to the effective date of revocation will not be retrospectively removed, due to the technical infeasibility and the aggregated nature of the trained AI Model. However, no new Anonymized Data from the Customer will be added.

8. INTELLECTUAL PROPERTY

8.1 The Customer retains all its existing rights, title, and interest in and to its data. 8.2 ISARR shall own all rights, title, and interest, including all intellectual property rights, in and to the AI Model, the Training Data Pool (as an aggregated and anonymized dataset), and any insights, analytics, or derivative works created or generated by ISARR from the AI Model and the Training Data Pool.

9. LIMITATION OF LIABILITY

9.1 ISARR's liability in connection with this AI Annex shall be subject to the limitations and exclusions of liability set out in the Main Agreement. 9.2 Without prejudice to the generality of the foregoing, ISARR provides the AI Model and any insights generated therefrom on an "as is" basis and makes no warranties, express or implied, regarding its accuracy, completeness, fitness for a particular purpose,

or non-infringement. The Customer acknowledges that any reliance on insights from the AI Model is at its own risk.

10. TERM AND TERMINATION
10.1 This AI Annex shall commence on the date of acceptance by the Customer and shall continue for the duration of the Main Agreement, unless terminated earlier in accordance with Clause 7 (Revocation of Consent) of this AI Annex. 10.2 Termination of the Main Agreement shall automatically terminate this AI Annex.

11. GENERAL
11.1 This AI Annex shall be governed by and construed in accordance with English law, and the parties submit to the jurisdiction of the English Courts. 11.2 This AI Annex, together with the Main Agreement (into which it is incorporated), constitutes the entire agreement between the parties concerning the subject matter hereof and supersedes all prior agreements, proposals, or communications, oral or written. 11.3 Any amendments to this AI Annex must be in writing and signed by authorised representatives of both parties. 11.4 If any provision of this AI Annex is held to be invalid, illegal, or unenforceable, the validity, legality, and enforceability of the remaining provisions shall not in any way be affected or impaired thereby.

IN WITNESS WHEREOF, the parties have indicated their acceptance of the terms of this AI Model Training Data Opt-In Agreement:

For [Insert Customer Company Name]:
By signing below, or by otherwise indicating affirmative consent through an ISARR-provided mechanism, the Customer agrees to the terms of this AI Model Training Data Opt-In Agreement.

Signature: _____
Name: _____ *(Print Name)*
Title: _____
Date: _____

For ISARR (Comunis Limited):
Signature: _____
Name: Nick Beale
Title: Managing Director
Date: _____