

Data Processing Agreement

ONSIM LTD

Version: v202608 Last updated: 21 August 2026

This Data Processing Agreement (“**DPA**”) is entered into between ONSIM LTD (company number 08429703, registered office 86-90 Paul Street, London, EC2A 4NE, United Kingdom) (“**ONSIM**”, “we”, “us”, “our”) and the customer identified in the Customer Terms (the “**Customer**”, “you”, “your”).

This DPA forms part of, and is incorporated into, the Customer Terms. It records the terms on which we process personal data on your behalf when we provide the Services, as required by Article 28 of the UK GDPR. Where there is any conflict between this DPA and the Customer Terms in relation to the processing of personal data, this DPA prevails.

This executed copy records the same terms as the version published at onsim.uk/dpa. Where the published version is later amended in accordance with clause 17, the amended version applies unless the parties agree otherwise in writing. If your procurement process requires a countersigned copy, contact privacy@onsim.uk and we will provide one.

1. Definitions

Terms used but not defined in this DPA have the meaning given in the UK GDPR or the Customer Terms.

Term	Definition
“ AI Insights ”	ONSIM’s optional add-on service that produces machine-generated transcripts and derived analysis from recorded calls.
“ Customer Terms ”	ONSIM’s terms and conditions for the provision of the Services, published at onsim.uk/terms , together with any order form, schedule or policy incorporated into them.
“ Customer Data ”	all data that the Customer, its users or its end users submit to, generate through, or that ONSIM generates in the course of providing, the Services, including call and message records, recordings, transcripts, configuration and account data.
“ Customer Personal Data ”	personal data contained within Customer Data that ONSIM processes on behalf of the Customer in providing the Services.

Term	Definition
“Data Protection Laws”	all laws relating to data protection and privacy applicable to a party, including the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (“ PECR ”), and, where applicable to a party, the EU GDPR, in each case as amended or replaced from time to time (including by the Data (Use and Access) Act 2025).
“EU GDPR”	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
“Interconnect Partner”	a licensed communications provider to which ONSIM hands off, or from which ONSIM receives, a call or message for onward transmission, and which determines for itself how it carries and records that traffic.
“Network Supplier”	a communications provider that supplies underlying network capability to ONSIM under contract, including host mobile radio access, mobile core connectivity and number range hosting, and which handles Customer Personal Data in doing so.
“Restricted Transfer”	a transfer of personal data to a country or territory outside the United Kingdom that is subject to Chapter V of the UK GDPR.
“Services”	the electronic communications and related services provided by ONSIM under the Customer Terms.
“Sub-processor”	any third party engaged by ONSIM to process Customer Personal Data on ONSIM’s behalf and on ONSIM’s instructions in the provision of the Services. It does not include an Interconnect Partner (see clause 3.4).
“Supervisory Authority”	the Information Commissioner and any successor body, including the Information Commission once the transfer of functions under Part 6 of the Data (Use and Access) Act 2025 takes effect.
“UK GDPR”	Regulation (EU) 2016/679 as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

The terms “**controller**”, “**processor**”, “**data subject**”, “**personal data**”, “**personal data breach**”, “**processing**” and “**special categories of personal data**” have the meanings given to them in the UK GDPR.

Any reference in this DPA to a repealed or superseded legal instrument is to be read as a reference to its successor.

2. Scope and instructions

2.1 ONSIM provides the Services to the Customer under the Customer Terms. In doing so, ONSIM processes Customer Data, which includes personal data.

2.2 ONSIM will process Customer Personal Data only to the extent necessary to provide the Services in accordance with the Customer Terms, this DPA and the Customer’s documented instructions.

2.3 The Customer’s initial documented instructions are set out in the Customer Terms, this DPA (including Annex 1) and the configuration the Customer applies through the ONSIM portal and API. The Customer may give further written instructions at any time. ONSIM will implement them where it is lawful and technically feasible to do so, and may charge for non-standard work in accordance with clause 15. If ONSIM cannot implement an instruction, it will tell the Customer promptly and the Customer may terminate the affected Services.

2.4 The subject matter, duration, nature and purpose of the processing, the types of personal data, the categories of data subjects and the obligations and rights of the Customer as controller are set out in **Annex 1**.

2.5 **No use for ONSIM’s own purposes.** ONSIM will not sell Customer Personal Data, use it for its own marketing, or use it to build, train, fine-tune or improve any artificial intelligence or machine learning model. Where AI Insights is enabled, transcription is performed by a Sub-processor under contractual terms that prohibit the use of Customer content for model training or service improvement.

3. Roles of the parties

3.1 **The Customer is the controller and ONSIM is the processor** in respect of Customer Personal Data, which is the personal data contained in and generated by the Customer’s use of the Services. This includes call and message content where recording is enabled, and the call and message records relating to the Customer’s users and the parties they communicate with.

3.2 **ONSIM acts as an independent controller** only in respect of:

- the account, billing, credit and contact data of the Customer and its authorised representatives, which we process to operate our business and comply with our legal obligations. That processing is described in our [Privacy Policy](#); and

- data we are required to generate, retain or disclose under our own regulatory obligations as a communications provider, including under PECR, the Communications Act 2003 and the Investigatory Powers Act 2016.

Where we act as an independent controller, this DPA does not apply and we are responsible for that processing in our own right. Some data has a dual character: call detail records, for example, are processed as processor to provide the Services and are separately retained by ONSIM as controller for billing, regulatory and statutory purposes under clause 14.6. ONSIM does not process call recordings, transcripts or message content as its own controller data, and will not do so unless a specific legal obligation requires it.

3.3 Where the Customer is itself a processor. If the Customer uses the Services to provide a service to its own customers and is acting as a processor rather than a controller, this DPA applies as between the Customer and ONSIM as if references to the Customer as controller were references to the Customer acting on the instructions of its own controllers. The Customer warrants that it has authority from those controllers to appoint ONSIM as a sub-processor and to agree this DPA on their behalf.

3.4 Interconnect Partners are not Sub-processors. Delivering a call or message requires ONSIM to hand traffic to other licensed communications providers, both in the UK and internationally. Those providers do not process personal data on ONSIM's instructions. They carry the communication under their own regulatory duties and act as independent controllers in respect of the data they receive and generate. This is inherent in the provision of any electronic communications service and is not sub-processing for the purposes of Article 28 of the UK GDPR. Because they are selected by the destination the Customer's user dials rather than by ONSIM, Interconnect Partners cannot be listed individually.

3.5 Network Suppliers are Sub-processors and are listed in Annex 3. The distinction between a Network Supplier and an Interconnect Partner is that ONSIM contracts with and selects a Network Supplier to deliver the Services, whereas an Interconnect Partner is determined by where the communication is going. A Network Supplier may also hold its own regulatory duties in respect of the traffic it carries, and acts as an independent controller to the extent it does so. That does not affect its status as a Sub-processor for the processing it carries out on ONSIM's instructions.

3.6 The Customer is responsible for determining the purposes and means of its own processing, including whether to enable call or SMS recording, what it records, who it gives access to, and what it does with recordings and transcripts once delivered.

4. ONSIM's obligations as processor

ONSIM will:

4.1 Documented instructions. Process Customer Personal Data only on the Customer's documented instructions, including in relation to a Restricted Transfer, unless required to do otherwise by law to which ONSIM is subject. Where ONSIM is required by law to process Customer Personal Data otherwise than on the Customer's instructions, ONSIM will inform the

Customer of that legal requirement before processing, unless the law prohibits it from doing so on important grounds of public interest (see also clause 10).

4.2 Unlawful instructions. Immediately inform the Customer if, in ONSIM's opinion, an instruction infringes the UK GDPR or other Data Protection Laws. ONSIM is not obliged to provide legal advice and is not responsible for the Customer's compliance with its own obligations as controller.

4.3 Confidentiality. Ensure that every person authorised to process Customer Personal Data is subject to a binding contractual duty of confidentiality or an appropriate statutory obligation of confidentiality, and that access is limited to those who need it to perform their role.

4.4 Personnel. Ensure that employees, agents and contractors who handle Customer Personal Data are made aware of its confidential nature and receive appropriate training on their data protection responsibilities.

4.5 Security. Implement and maintain the technical and organisational measures set out in **Annex 2**, in accordance with Article 32 of the UK GDPR.

4.6 Sub-processors. Comply with clause 6 in engaging any Sub-processor.

4.7 Data subject rights. Assist the Customer in accordance with clause 8.

4.8 Security, breach, impact assessment and consultation. Assist the Customer, taking into account the nature of the processing and the information available to ONSIM, in complying with its obligations under Articles 32 to 36 of the UK GDPR, in accordance with clauses 4.5, 11 and 12.

4.9 Deletion and return. Delete or return Customer Personal Data in accordance with clause 14.

4.10 Records and demonstrating compliance. Maintain a record of processing carried out on behalf of the Customer in accordance with Article 30(2) of the UK GDPR, make available to the Customer all information necessary to demonstrate compliance with Article 28 of the UK GDPR, and allow for and contribute to audits in accordance with clause 13.

5. The Customer's obligations as controller

5.1 The Customer warrants that it will comply with Data Protection Laws in its use of the Services, and that it has a lawful basis for the processing it instructs ONSIM to carry out.

5.2 Recording and monitoring. Where the Customer enables call or SMS recording, the Customer is solely responsible for:

- establishing and documenting a lawful basis for recording and for any subsequent transcription or analysis;
- providing the notice and transparency information required by Articles 13 and 14 of the UK GDPR to its own staff and to the parties they communicate with;

- complying with PECR and the Investigatory Powers Act 2016 in relation to the interception and recording of communications;
- carrying out a data protection impact assessment where one is required; and
- determining and applying its own retention period to recordings and transcripts once they are delivered to it.

Other than automated transcription and analysis performed at the Customer's instruction where AI Insights is enabled, ONSIM does not monitor, review or assess the content of recordings, transcripts or messages.

5.3 Special category data. The Customer must not use the Services in a way that requires ONSIM to process special categories of personal data or personal data relating to criminal convictions and offences as a deliberate or systematic feature of the Services, without first agreeing this in writing with ONSIM. The Customer acknowledges that call and message content may incidentally contain such data, and that ONSIM cannot identify or segregate it.

5.4 The Customer is responsible for the accuracy of the personal data it provides, for the security and administration of its own account credentials, and for controlling which of its users can access recordings, transcripts and call records.

5.5 The Customer must ensure that any of its affiliates or group companies that use the Services comply with the Customer's obligations under this DPA, and is liable for their acts and omissions as if they were its own.

6. Sub-processors

6.1 General authorisation. The Customer gives ONSIM general written authorisation to engage Sub-processors to process Customer Personal Data in providing the Services. Every Sub-processor engaged at the date of this DPA is listed in **Annex 3**, by the role it performs, the categories of data it processes, where it processes them and the transfer mechanism relied on. The identity of each Sub-processor is confidential and is provided to the Customer on request under clause 6.5.

6.2 Changes and objection. ONSIM will give the Customer at least **30 days' notice**, by email to the account contact and by publishing an updated Annex 3, before authorising a new or replacement Sub-processor to process Customer Personal Data. The notice will state the role, the categories of data, the location of processing and the transfer mechanism, and will give the identity of the Sub-processor on request under clause 6.5. The Customer may object within that period. If it does, the parties will discuss the objection in good faith. If ONSIM cannot provide the affected part of the Services without the Sub-processor and the objection is not resolved within 30 days, the Customer may terminate the affected Services without penalty and ONSIM will refund any prepaid fees covering the period after termination.

6.3 Flow-down. ONSIM will impose on each Sub-processor, by written contract, data protection obligations that are materially the same as those set out in this DPA, and in particular the obligations required by Article 28(3) of the UK GDPR.

6.4 Liability. ONSIM remains liable to the Customer for the performance of each Sub-processor's obligations to the same extent as if ONSIM were performing those services itself, as required by Article 28(4) of the UK GDPR. The financial limits in clause 16 apply to that liability in the same way as they apply to ONSIM's own acts and omissions.

6.5 Identity of Sub-processors. On written request, and at no charge, ONSIM will provide the Customer with the name, registered address, country of processing and a data protection contact point for every Sub-processor, and, where the Customer needs it to meet its own accountability obligations, a copy of the relevant sub-processing terms with commercial terms redacted. ONSIM will respond within 10 business days.

The identity of ONSIM's Sub-processors is commercially sensitive and is ONSIM's confidential information. The Customer may use and disclose it only for the purpose of meeting its own obligations under Data Protection Laws, and may disclose it to its professional advisers, its auditors, a Supervisory Authority, and any controller on whose behalf it acts under clause 3.3, in each case on terms of confidentiality. This does not restrict the Customer from disclosing anything it is required by law to disclose, or anything already in the public domain other than through the Customer's breach of this clause. ONSIM will not withhold the information for any reason other than the Customer's refusal to accept this obligation.

6.6 Continuity substitution. Where an existing Sub-processor fails, withdraws its service or suffers a security compromise, and ONSIM must engage a replacement to maintain continuity or security of the Services, ONSIM may do so before the notice period in clause 6.2 has expired. ONSIM will notify the Customer within **5 business days** and clause 6.2 will then apply from the date of that notice. During any objection period the Customer may require ONSIM to suspend the transfer of the Customer's data to the replacement Sub-processor. Where that is not technically possible without suspending the affected Services, ONSIM will tell the Customer and the Customer may suspend or terminate those Services without penalty.

7. International transfers

7.1 Where data is held. Call and SMS recordings, transcripts and call detail records relating to the Customer are stored at rest in the United Kingdom. Some Sub-processors access or process Customer Personal Data from outside the United Kingdom, including remote engineering support access, and some categories of Customer Personal Data are processed outside the United Kingdom. Each instance is identified in **Annex 3**, together with the transfer mechanism relied on. Remote access from outside the United Kingdom is treated as a Restricted Transfer and is subject to clause 7.2.

7.2 ONSIM will not make a Restricted Transfer of Customer Personal Data, and will not permit a Sub-processor to do so, unless one of the following applies:

- the transfer is to a country or territory approved by regulations made under **Article 45A of the UK GDPR**;
- the transfer is made under the ICO's International Data Transfer Agreement (IDTA), or the International Data Transfer Addendum to the European Commission's Standard Contractual Clauses, in each case in the version issued by the Information

Commissioner and in force from time to time, and supported by a transfer risk assessment carried out against the data protection test in Article 46(1A) and (6) of the UK GDPR; or

- another appropriate safeguard under Article 46, or a derogation under Article 49, of the UK GDPR applies.

ONSIM will provide the Customer with a copy of the relevant transfer risk assessment on written request.

7.3 International calls and messages. Where the Customer's user makes or receives an international call or message, delivering that communication necessarily involves disclosing the calling and called numbers, routing data and the content of the communication to communications providers outside the United Kingdom. That disclosure is made in reliance on **Article 49(1)(b) of the UK GDPR** where the data subject is the Customer's own user, the transfer being necessary for the performance of a contract concluded at that data subject's request, and on **Article 49(1)(c)** in respect of the other party to the communication, the transfer being necessary for the conclusion or performance of a contract concluded in that data subject's interest. It is inherent in any international telephony service and cannot be avoided while the Service is used to communicate internationally. The Customer should reflect this in its own transparency information.

7.4 EU and EEA customers. Where the Customer is established in the EEA and the EU GDPR applies to its processing, ONSIM processes Customer Personal Data in the United Kingdom, which benefits from the European Commission's adequacy decision for the United Kingdom (Implementing Decision (EU) 2021/1772, as amended by Implementing Decision (EU) 2025/2574 and in force until 27 December 2031). If that adequacy decision lapses or is annulled, the parties will without undue delay put in place the European Commission's Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), Module Two (controller to processor), which are deemed incorporated into this DPA on that date with ONSIM as data importer, this DPA and its Annexes 1 and 2 populating Annexes I and II of those Clauses, the named Sub-processor list provided under clause 6.5 populating Annex III, and the law and courts of Ireland selected under clauses 17 and 18 of those Clauses.

7.5 The Customer must not instruct ONSIM to make a Restricted Transfer other than as set out in this clause 7.

8. Data subject rights

8.1 If ONSIM receives a request from a data subject to exercise rights under Chapter III of the UK GDPR in relation to Customer Personal Data, ONSIM will not respond to the request itself, other than to acknowledge it and direct the data subject to the Customer, unless required to respond by law or instructed by the Customer to do so. ONSIM will notify the Customer of the request without undue delay.

8.2 Taking into account the nature of the processing, ONSIM will assist the Customer by appropriate technical and organisational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to such requests. Much of this can be done by the Customer

directly through the ONSIM portal and API, and the Customer will use that functionality where it is available.

8.3 The parties acknowledge that under Article 15(1A) of the UK GDPR, as inserted by section 78 of the Data (Use and Access) Act 2025, a data subject is entitled only to such personal data as can be found following a **reasonable and proportionate search**. ONSIM's assistance obligation is limited accordingly.

8.4 Where the Customer has paused or extended a response period pending verification of identity or clarification of a request, ONSIM's assistance obligation runs from the date the Customer notifies ONSIM that the request has been verified or clarified.

8.5 Assistance under this clause is provided at no charge where it can be met using the standard functionality of the Services. ONSIM may charge in accordance with clause 15 only for assistance requiring non-standard engineering work, and will quote in advance.

9. Complaints

9.1 If ONSIM receives a complaint about the processing of Customer Personal Data, ONSIM will forward it to the Customer without undue delay and will not respond to it substantively, unless required to do so by law.

9.2 ONSIM will provide the Customer with reasonable assistance in meeting its obligations under section 164A of the Data Protection Act 2018, including the requirement to acknowledge a complaint within 30 days.

9.3 ONSIM will notify the Customer promptly of any request, complaint or communication from a Supervisory Authority that relates to the processing of Customer Personal Data, unless prohibited by law or court order.

9.4 Each party will cooperate, on request, with a Supervisory Authority in the performance of its obligations under this DPA.

10. Government and law enforcement requests

10.1 If ONSIM receives a legally binding request from a public authority, law enforcement body or court for disclosure of Customer Personal Data, ONSIM will notify the Customer before disclosing, so that the Customer can seek to challenge the request, **except** where ONSIM is prohibited from giving that notice by law, including under the Investigatory Powers Act 2016, or where the request relates to an imminent risk to life.

10.2 Where ONSIM is prohibited from notifying the Customer, ONSIM will take reasonable steps, including seeking legal advice where appropriate, to have the prohibition lifted or narrowed, and to challenge any request that is manifestly unlawful or excessive.

10.3 ONSIM will disclose only the minimum data specified in the request.

10.4 The Customer acknowledges that as a UK communications provider, ONSIM is subject to statutory obligations relating to the retention of communications data, lawful interception and technical capability, and that ONSIM's compliance with those obligations is not a breach of this DPA.

11. Personal data breach

11.1 ONSIM will notify the Customer **without undue delay, and in any event within 48 hours**, after becoming aware of a personal data breach affecting Customer Personal Data. Notification will be sent to the Customer's registered account contact and to any additional security contact the Customer has provided.

11.2 **When ONSIM becomes aware.** ONSIM becomes aware of a personal data breach when it has a reasonable degree of certainty that a security incident has occurred that has led to Customer Personal Data being compromised. An alert, an anomaly or an unverified report is not by itself awareness. ONSIM will investigate any such indication promptly, and that short initial period of investigation forms part of, and does not extend, the time in clause 11.1.

11.3 **Phased notification.** Where ONSIM cannot provide all of the information in clause 11.4 at once, it will provide what it has within the period in clause 11.1 and supply the remainder in phases without further undue delay, as permitted by Article 33(4) of the UK GDPR. An initial notification given in good faith with the information then available satisfies clause 11.1.

11.4 The notification will describe, to the extent known at the time and updated as further information becomes available:

- the nature of the breach, including where possible the categories and approximate number of data subjects and records concerned;
- the name and contact details of ONSIM's contact point for further information;
- the likely consequences of the breach; and
- the measures taken or proposed to address the breach and mitigate its effects.

11.5 ONSIM will take all commercially reasonable measures to secure the affected data, limit the effects of the breach, investigate the cause and assist the Customer in meeting its own obligations under Articles 33 and 34 of the UK GDPR, including by identifying which of the Customer's records are affected.

11.6 **ONSIM's own regulatory notification duty.** Where ONSIM is a provider of a public electronic communications service, regulation 5A of PECR requires it to notify the Information Commissioner of a personal data breach without undue delay and, where feasible, within 72 hours, giving reasons for any delay beyond that period, and in certain cases to notify affected subscribers and users. That duty is ONSIM's own and does not depend on the Customer's consent or instruction. Each party will inform the other of any notification it intends to make to a Supervisory Authority or to data subjects in relation to the same breach, but neither party's duty to notify is conditional on the other's agreement. ONSIM maintains a breach inventory in accordance with regulation 5A(8) of PECR.

11.7 ONSIM's notification of, or response to, a breach is not an acknowledgement of fault or liability.

11.8 ONSIM does not review the substantive content of recordings, transcripts or messages in order to assess a breach. Subject to ONSIM's assistance under clause 11.5, the Customer is responsible for meeting its own notification obligations to data subjects and third parties.

12. Impact assessments and prior consultation

12.1 ONSIM will provide the Customer, on written request, with the information about the Services reasonably required for the Customer to carry out a data protection impact assessment under Article 35 of the UK GDPR, or to consult a Supervisory Authority under Article 36. This includes the information in Annexes 1, 2 and 3, ONSIM's data flow and retention information, and answers to a reasonable security and privacy questionnaire.

12.2 Automated decision-making. ONSIM does not take decisions producing legal or similarly significant effects concerning data subjects on the Customer's behalf. Where AI Insights is enabled, ONSIM produces transcripts and analysis but does not act on them. Any decision taken using that output is the Customer's, and the Customer is responsible for the safeguards required by Article 22C of the UK GDPR.

12.3 Fraud and abuse controls. ONSIM operates automated fraud and abuse controls that may bar destinations or suspend a service on suspected compromise. These are network protection measures taken by ONSIM as a communications provider in its own right under clause 3.2, are applied to accounts and routes rather than to individuals, and are reviewable by a person on request to ONSIM support.

13. Audit

13.1 ONSIM will make available to the Customer all information necessary to demonstrate compliance with Article 28 of the UK GDPR, and will allow for and contribute to audits and inspections conducted by the Customer or an auditor it mandates, in accordance with the procedure in this clause 13.

13.2 Documentation route. The Customer's audit right is exercised in the first instance by ONSIM providing its current certifications, security documentation, most recent external vulnerability assessment summary, the information in Annexes 1, 2 and 3, and responses to a reasonable security questionnaire. ONSIM will respond within 30 days of a written request, **at no charge**, once in any 12 month period and additionally following any personal data breach affecting the Customer.

13.3 On-site and remote audits. Where the Customer, acting reasonably, considers that the information provided under clause 13.2 is not sufficient to demonstrate compliance, it may conduct an on-site or remote audit. Before doing so the Customer must identify in writing which specific matters it has been unable to verify from that information and why. ONSIM will

first seek to resolve those matters by providing further information, and an audit under this clause will proceed only to the extent they remain unresolved.

13.4 An audit under clause 13.3 will be:

- limited in scope to the matters identified under clause 13.3 and to ONSIM's processing of that Customer's Personal Data;
- carried out during UK business hours on not less than 30 days' written notice, with the scope, timing, personnel and method agreed in advance in writing;
- conducted no more than once in any 12 month period;
- conducted remotely where that is capable of achieving the audit's purpose;
- conducted by the Customer's own personnel or by an independent auditor it mandates, who must be bound by appropriate confidentiality obligations and must not be a competitor of ONSIM;
- conducted under ONSIM supervision, without access to the personal data, systems, premises or documentation of any other customer, and without access to ONSIM's source code, commercial terms with suppliers, or pricing information; and
- conducted in a way that does not interfere with the security or availability of the Services for ONSIM's other customers.

ONSIM may refuse access to any individual auditor on reasonable grounds and may require an alternative to be nominated.

13.5 **Costs.** The Customer bears its own costs of any audit under clause 13.3 and will reimburse ONSIM for its reasonable time, costs and expenses in preparing for and supporting the audit, charged at ONSIM's standard professional services rates and quoted in advance. **No charge applies where** the audit follows a personal data breach affecting the Customer, is required by a Supervisory Authority, or identifies a material breach by ONSIM of this DPA or of Data Protection Laws.

13.6 Nothing in this clause 13 limits or delays the exercise by a Supervisory Authority, or by a regulator to whose supervision the Customer is subject, of any statutory power of audit, inspection or access. Where the Customer is required by law or by such a regulator to audit more frequently or on shorter notice than this clause provides, the parties will agree a reasonable approach in good faith.

13.7 The Customer must treat all information obtained through an audit as ONSIM's confidential information, and must not disclose it except as required by law, or to its professional advisers, a Supervisory Authority, or any controller on whose behalf the Customer acts under clause 3.3.

13.8 This clause 13 sets out the agreed procedure for exercising the audit right in Article 28(3) (h) of the UK GDPR.

14. Retention, return and deletion

14.1 During the term. The Customer may delete Customer Personal Data using the functionality provided in the Services. ONSIM may retain deleted data for a recovery period of up to 90 days to allow recovery from accidental deletion, after which it is permanently deleted from live systems.

14.2 Recordings and transcripts. Where the Customer uses call or SMS recording, recordings and transcripts are delivered to the Customer, including by SFTP where the Customer has configured it. Retention on ONSIM systems is the period configured on the Customer's account, which the Customer can view and change in the ONSIM portal. Where no period has been configured, recordings and transcripts are deleted from ONSIM systems 90 days after they are created, or on confirmed SFTP delivery to the Customer, whichever is earlier. Once delivered, the Customer is responsible for retention and deletion of its own copies.

14.3 On termination. At the Customer's choice, ONSIM will return or delete Customer Personal Data. The Customer may request return, in a commonly used machine readable format, at any time up to 30 days after termination or expiry of the Customer Terms; one such export is provided at no charge. **Whether or not the Customer makes a request, ONSIM will permanently delete Customer Personal Data from live systems within 30 days of termination or expiry, or within 10 days of completing an export, whichever is later.**

14.4 Backups and archives. Following deletion from live systems, residual copies may persist in backup and archival systems for **no more than 90 further days** before being overwritten in the ordinary course. On termination this means Customer Personal Data is erased from live systems within the period in clause 14.3, and from all backup and archival systems within 90 days after that. Backup copies remain subject to this DPA, including clauses 4.3, 4.5, 7 and 11, until they are deleted.

14.5 Certificate of deletion. ONSIM will provide written confirmation of deletion on request.

14.6 Statutory retention. ONSIM may retain specific categories of data where required or permitted to do so by law, and only for as long as that requirement lasts, namely:

- traffic and billing data, under regulation 7(2) of PECR, for the purpose of subscriber billing and interconnect payments, subject to the limits in regulation 7(5);
- communications data specified in a retention notice given under Part 4 of the Investigatory Powers Act 2016;
- invoicing, tax and accounting records required under the Companies Act 2006 and tax legislation; and
- data required to establish, exercise or defend legal claims, retained for no longer than the applicable limitation period.

Call recordings, transcripts and message content are **not** retained under this clause unless a specific legal obligation requires it, in which case ONSIM will inform the Customer unless prohibited by law. Data retained under this clause is not further processed for any other purpose and remains protected by the measures in Annex 2.

15. Charges for assistance

Where the Customer requests assistance under this DPA that goes beyond ONSIM's standard operational procedures, including audits under clause 13.3, ONSIM may charge for its reasonable staff time, costs and expenses, notified in advance. ONSIM will not charge for assistance it is required by law to provide free of charge, nor for anything this DPA states is provided at no charge.

16. Liability

16.1 The limitations and exclusions of liability in the Customer Terms apply to all claims arising under or in connection with this DPA.

16.2 Nothing in this DPA or the Customer Terms limits either party's liability to a data subject or a Supervisory Authority, or any liability that cannot be limited by law.

16.3 Neither party may recover more than once in respect of the same loss.

16.4 ONSIM maintains cyber and professional indemnity insurance appropriate to the scale of the Services, and will provide evidence of cover on request.

17. Changes to this DPA

17.1 ONSIM may amend this DPA where necessary to reflect a change in Data Protection Laws or in guidance issued by a Supervisory Authority. ONSIM will publish the amended DPA at onsim.uk/dpa and give the Customer at least 30 days' notice by email to the account contact.

17.2 Changes to Annex 3 are governed by clause 6.2. ONSIM will give the Customer at least 30 days' notice of any change to Annex 2 that materially reduces the level of security.

17.3 If the Customer reasonably objects to an amendment under clause 17.1, the parties will discuss it in good faith. If it is not resolved within 30 days, the Customer may terminate the affected Services without penalty and ONSIM will refund any prepaid fees for the period after termination.

18. Term and general

18.1 This DPA takes effect on the commencement of the Customer Terms and terminates on their termination or expiry, except that:

- clauses 2.5, 4.3, 4.5 (together with Annex 2), 6.3, 7, 8, 10, 11, 13 and 14 continue to apply for as long as ONSIM or any Sub-processor holds any Customer Personal Data; and
- the confidentiality obligations in clauses 6.5 and 13.7, and clauses 16 and 18, continue to apply without limit of time.

18.2 This DPA, together with the Customer Terms, sets out the entire understanding of the parties in relation to the processing of Customer Personal Data. Where there is a conflict, the order of precedence is: (i) the clauses of this DPA; (ii) Annex 1; (iii) Annex 3; (iv) Annex 2; (v) the Customer Terms.

18.3 If any provision of this DPA is or becomes invalid, the remaining provisions are unaffected, and the invalid provision is to be replaced by a valid provision that comes closest to the parties' commercial intention.

18.4 This DPA is governed by the laws of England and Wales, and the courts of England and Wales have exclusive jurisdiction over any dispute arising under it, subject to clause 7.4.

Annex 1: Details of processing

Required by Article 28(3) of the UK GDPR.

Subject matter

ONSIM's provision of the Services to the Customer under the Customer Terms.

Duration

The term of the Customer Terms, plus the deletion and retention periods in clause 14.

Nature of the processing

Collection, recording, organisation, storage, transmission, retrieval, consultation, use, transcription (where AI Insights is enabled), disclosure by transmission, restriction, erasure and destruction, carried out by automated means.

Purpose of the processing

Provision of electronic communications services, comprising: number provisioning, porting and hosting; routing, switching and delivery of voice calls; delivery of SMS and messaging; SIM and eSIM provisioning and mobile connectivity; presentation of calling line identity; call forwarding and diversion; voicemail; generation of call detail records; call and SMS recording and delivery where enabled by the Customer; transcription and analysis where AI Insights is enabled by the Customer; provision of the customer portal and API; and fault management and technical support.

Frequency

Continuous, for the duration of the Customer Terms.

Obligations and rights of the Customer

As set out in clause 5 of this DPA and in the

Customer Terms.

Types of personal data

- Identity and contact data of the Customer's users and authorised administrators: name, business email address, job title, telephone number
- Service identifiers: allocated telephone numbers, SIM and eSIM identifiers (ICCID, IMSI), device identifiers (IMEI), account and sub-account identifiers, portal usernames
- Installation and registration address data, including addresses provided to the emergency services database and to number porting processes
- **Traffic data**: calling and called numbers, date, time and duration of calls and messages, call direction, routing and interconnect data, delivery status, data usage records
- **Location data** to the extent generated by the mobile network in the course of providing the Services
- Technical data: IP addresses, signalling and session data, portal and API access logs
- **Content data**, where the Customer enables it: call recordings, SMS and message content, voicemail messages, and transcripts and derived analysis produced by AI Insights
- Support data: the contents of support tickets, correspondence and fault reports raised by or about the Customer's users

ONSIM does not require, request or intentionally process special categories of personal data. The Customer acknowledges that content data may incidentally contain such data (see clause 5.3).

Categories of data subjects

- The Customer's employees, workers, contractors and authorised administrators
- End users to whom the Customer allocates a number, SIM or eSIM
- Individuals who call, are called by, message or are messaged by the Customer's users, including the Customer's own customers, suppliers and contacts
- Individuals whose personal data appears in the content of a recorded call or message

Retention periods

Category	Retention on ONSIM systems
Call and message detail records, available to the Customer in the portal and API	90 days from the date of the record, unless a longer period is agreed
Call and message detail records retained by ONSIM as controller for billing, dispute and statutory purposes	6 years, under clause 14.6
Call and SMS recordings and transcripts	The period configured on the Customer's account, or the default in clause 14.2 where none is configured
Account, service identifier and configuration data	Duration of the Customer Terms, then per clause 14.3
Support tickets and correspondence	24 months from closure of the ticket

Category	Retention on ONSIM systems
Billing and invoicing records	6 years, retained by ONSIM as controller under clause 14.6
Portal and API access logs	12 months

Recipients

Customer Personal Data is disclosed to: the Sub-processors in Annex 3; Interconnect Partners, for the purpose of delivering communications (clause 3.4); the operator of the UK emergency services database, where the Customer provides an address for that purpose; gaining and losing communications providers, where a number is ported; and public authorities where required by law (clause 10).

Annex 2: Technical and organisational measures

Required by Article 32 of the UK GDPR. These measures are subject to ongoing development and review. ONSIM may adopt alternative measures provided they do not reduce the overall level of security of the Services, and will give notice of any material reduction under clause 17.2.

Governance and certification

- ONSIM holds **Cyber Essentials** certification, renewed annually
- Written information security, acceptable use and data protection policies, reviewed at least annually
- ONSIM is registered with the Information Commissioner's Office as both a controller and a processor
- A named point of accountability for data protection at director level

Access control

- Call and SMS recordings are encrypted at rest. **Decryption keys are held by a small number of named senior individuals under a documented break-glass procedure.** Access is granted only for a defined purpose, such as investigating a fault or a security incident, is approved in advance and is logged
- **Customer support personnel hold no decryption keys and do not access recording content** in the course of normal support work. Access to recording content is restricted to the named key holders under the procedure above
- Role based access control and least privilege across platform, portal and infrastructure
- Multi-factor authentication on administrative and infrastructure access
- Individual named accounts, with no shared credentials for privileged access
- Access reviewed on change of role and revoked on termination of employment
- Logical separation of customer data by tenant, so that one customer's data is not accessible from another customer's account

Encryption and pseudonymisation

- Encryption in transit for portal, API and file transfer, including TLS for web and API traffic and SFTP for the delivery of recordings and transcripts
- Encryption at rest for stored call and SMS recordings and transcripts
- Key management procedures covering generation, storage, rotation and recovery, so that loss of an individual key holder does not render Customer Personal Data unrecoverable
- Signalling and media security applied in line with the capabilities of the underlying network and the Customer's configuration

Infrastructure and network security

- Services hosted in UK data centre regions operated by providers holding recognised security certifications, with physical access controls, environmental protection and continuous monitoring
- Network segmentation between public facing, application and data layers
- Firewalling and session border control on voice signalling and media paths
- Fraud detection and monitoring on outbound traffic, with the ability to bar destinations and suspend accounts on suspected compromise
- Patch and vulnerability management on ONSIM managed systems
- Logging and monitoring of administrative access and security relevant events

Resilience, continuity and recovery

- Redundancy across core platform and media components
- Backup of platform and billing data, with documented and tested restoration procedures
- Documented incident response and escalation procedures, covering breach assessment, customer notification and regulatory notification
- Service status monitoring and customer notification of major incidents

Personnel

- **Front-line customer support is delivered in house by UK based ONSIM employees and is not outsourced or offshored.** Third-party vendor engineering support is provided only as set out in Annex 3
- Identity and right to work verification, and reference checks, before employment
- Confidentiality obligations in all employment and contractor agreements
- Data protection and security awareness training appropriate to role
- Documented joiner, mover and leaver process covering access provisioning and revocation

Supplier management

- Sub-processors assessed before engagement and bound by written data protection terms
- Sub-processor list maintained, published by role in Annex 3 with identities released to customers on request, and 30 days' notice given of changes

- Contractual prohibition on Sub-processors using Customer content to train or improve AI or machine learning models

Testing and assurance

- Annual Cyber Essentials recertification
- Annual external vulnerability assessment of internet-facing systems
- Periodic review of access rights, firewall rules and platform configuration
- Review of technical and organisational measures following any material change to the Services or any significant security incident

Regulatory security duties

As a UK communications provider, ONSIM is subject to the network and service security duties in sections 105A to 105D of the Communications Act 2003. ONSIM applies the principles of the Telecommunications Security Framework, including the code of practice issued by the Secretary of State under section 105E of that Act, as relevant to a provider of its size and tier.

Annex 3: Sub-processors

Annex 3 version: 21 August 2026

The following Sub-processors process Customer Personal Data on ONSIM's behalf. Each is identified by the role it performs. **The identity of each Sub-processor is provided to the Customer on request, at no charge, under clause 6.5**, on terms of confidentiality. It is not published because ONSIM's supply chain is commercially sensitive, and because the information a customer needs to assess risk is the role, the data, the location and the transfer mechanism, all of which are set out below.

Interconnect Partners are not Sub-processors and are not listed here (see clause 3.4).

#	Role	Data processed	Location and transfer mechanism
1	Core telephony platform vendor. Switching, rating, billing and call detail record platform, and vendor engineering support	Identity and contact data, service identifiers, traffic data, billing data	Platform hosted in the United Kingdom. Vendor support access from Canada, under UK adequacy regulations for Canada (PIPEDA)
2	Cloud infrastructure and speech-to-text provider. Hosting and storage of call and SMS recordings,	Content data, service identifiers, technical data	United Kingdom (London region). No Restricted Transfer

#	Role	Data processed	Location and transfer mechanism
	and transcription for AI Insights		
3	Mobile core connectivity provider (Network Supplier). SIM and eSIM provisioning, roaming and signalling	Service identifiers, traffic data, location data	United Kingdom and EEA, under UK adequacy regulations
4	UK host mobile network operator (Network Supplier). Radio access	Service identifiers, traffic data, location data	United Kingdom. No Restricted Transfer
5	UK inbound number range and non-geographic call carriage provider (Network Supplier)	Service identifiers, traffic data	United Kingdom. No Restricted Transfer
6	Card payment processor	Billing and contact data of the Customer's account holder	United Kingdom and EEA under adequacy; United States under the UK Extension to the EU-US Data Privacy Framework and the ICO International Data Transfer Addendum
7	Legacy subscription billing provider , for accounts not yet migrated to entry 6	Billing and contact data of the Customer's account holder	United States, under the ICO International Data Transfer Addendum to the EU Standard Contractual Clauses
8	Customer support ticketing and help centre provider	Identity and contact data, support data, service identifiers	EEA under adequacy; United States under the UK Extension to the EU-US Data Privacy Framework and the ICO International Data Transfer Addendum

Entries 6 and 7 process the billing and contact data of the Customer's account holder, which ONSIM also processes as controller under clause 3.2. They are listed here in full for transparency and are subject to the notification and objection rights in clause 6.2.

The adequacy regulations referred to above are those made under Article 45A of the UK GDPR, including regulations treated as so made by paragraph 26 of Part 2 of Schedule 9 to the Data (Use and Access) Act 2025.

Changes to this list are notified to account contacts by email at least 30 days in advance, in accordance with clause 6.2.

Contact

Questions about this DPA, security questionnaires, breach notifications and requests for a countersigned copy should be sent to:

Data Protection, ONSIM LTD 86-90 Paul Street, London, EC2A 4NE, United Kingdom
privacy@onsim.uk

See also our [Privacy Policy](#) and [Terms and Conditions](#).

Execution

This DPA is agreed by the parties on the dates set out below.

Signed for and on behalf of ONSIM LTD

Signature: _____

Name: _____

Position: _____

Date: _____

Signed for and on behalf of the Customer

Company name: _____

Company number: _____

Registered address: _____

Signature: _____

Name: _____

Position: _____

Date: _____

Customer contacts for the purposes of this DPA

Account contact, for sub-processor and DPA change notices (clauses 6.2 and 17.1):

Security contact, for personal data breach notification (clause 11.1):

Data protection contact:
