TERMS AND CONDITIONS

Data Processing Annexure

How FirstNet processes Customer Personal Information as an operator under POPIA

VERSION v2026.11a

EFFECTIVE 1 November 2026

This Data Processing Annexure sets out the terms on which FirstNet Technology Services (Pty) Ltd processes personal information on behalf of its customers. It forms part of the Agreement (the FirstNet Standard Terms and Conditions or the Customer's signed Master Services Agreement) and is referred to in every set of FirstNet Service Specific Terms.

1. Status and precedence

1.1 This Annexure applies whenever FirstNet processes Customer Personal Information as an operator for the Customer in providing a Service.

1.2 It does not apply to personal information that FirstNet processes as a responsible party for its own purposes (such as account management, billing, credit vetting, RICA registration, network security, fraud prevention and its own marketing). That processing is described in FirstNet's Privacy Notice at www.firstnet.co.za/privacy-policy/.

1.3 If this Annexure conflicts with another part of the Agreement on the processing of Customer Personal Information, this Annexure applies, unless the Service Specific Terms for a Service set stricter data requirements, which then apply to that Service.

1.4 If the Customer and FirstNet have signed a separate operator agreement or data processing agreement, that agreement applies instead of this Annexure to the extent of any conflict.

1.5 Words defined in the Agreement have the same meanings in this Annexure. Words defined in POPIA (such as "data subject", "operator", "personal information", "processing", "responsible party" and "special personal information") have their POPIA meanings.

2. Definitions

2.1 **"Customer Personal Information"** means personal information (as defined in POPIA) contained in Customer Data that FirstNet processes on behalf of the Customer as an operator (the same meaning as in the Standard Terms and Conditions).

2.2 **"Security Compromise"** means a situation where there are reasonable grounds to believe that Customer Personal Information has been accessed or acquired by an unauthorised person, as contemplated in section 22 of POPIA, while in the possession or under the control of FirstNet or a Sub-operator.

2.3 **"Sub-operator"** means a third party (including a Vendor or a FirstNet Affiliate) that FirstNet engages to process Customer Personal Information for a Service.

2.4 **"Sub-operator List"** means the list of Sub-operators in Annex B, as FirstNet updates it under clause 6.3, showing for each Sub-operator its name, the Services it supports, what it processes, where it processes data and the basis for any transfer outside South Africa.

3. Roles and instructions

3.1 The Customer is the responsible party for Customer Personal Information, and FirstNet is its operator. Where the Customer is itself an operator for another responsible party, the Customer confirms that it is authorised by that responsible party to appoint FirstNet as a further operator on these terms.

3.2 FirstNet will process Customer Personal Information only:

3.2.1 to provide, support, secure and maintain the Services in accordance with the Agreement;

3.2.2 in accordance with the Customer's documented instructions, which are the Agreement, the Service Schedule, the Customer's configuration of the Service and any further reasonable written instructions consistent with the Agreement; and

3.2.3 as required by Applicable Law (including a direction under RICA or a court order), in which case FirstNet will, where lawful, tell the Customer before processing.

3.3 FirstNet will tell the Customer if it believes an instruction breaches POPIA. FirstNet is not obliged to follow an instruction that would breach Applicable Law, and may charge reasonable costs for instructions that go beyond the scope of the Service.

3.4 Annex A describes the processing for each type of Service. The Service Specific Terms may describe it in more detail.

3.5 The Customer is responsible for:

3.5.1 having a lawful basis under section 11 of POPIA for the processing, and for giving its data subjects the notice required by section 18;

3.5.2 obtaining any consents required, including for the processing of special personal information or personal information of children, for direct marketing under section 69, for call recording and monitoring under RICA, and for cross-border transfers under section 72(1)(b) where the Customer relies on consent;

3.5.3 the accuracy and lawfulness of Customer Personal Information it gives FirstNet; and

3.5.4 the settings it chooses in a Service, including retention periods, access rights, encryption options and data location options.

4. Confidentiality

4.1 FirstNet will treat Customer Personal Information as confidential and will not disclose it except as allowed by this Annexure or the Agreement.

4.2 FirstNet will ensure that its employees and contractors who have access to Customer Personal Information are bound by confidentiality obligations, receive training on data protection, and have access only to what they need for their role.

5. Security measures (POPIA section 19)

5.1 FirstNet will maintain appropriate, reasonable technical and organisational measures to protect Customer Personal Information against loss, damage, unauthorised destruction and unlawful access or processing, having regard to generally accepted information security practices and the nature of the Service.

5.2 FirstNet operates an information security management system certified to ISO/IEC 27001:2022 by INTERCERT (certificate IC-IS-2512139). The certified scope is: "The Information Security Management System at FirstNet Technology Services (Pty) Ltd applies to the design, deployment, operation, and support of cloud, connectivity, voice, firewall, and security services, including all associated network infrastructure and technical operations." The measures FirstNet applies are summarised in Annex C. FirstNet will provide a copy of its current certificate on request.

5.3 FirstNet will regularly identify reasonably foreseeable risks to Customer Personal Information, maintain safeguards against them, verify that the safeguards are effective, and update them in response to new risks.

5.4 Security is shared. The Customer is responsible for the security of its own systems, credentials, administrator accounts and devices, for the configuration choices it controls, and for the security measures that the Service Specific Terms place on the Customer.

6. Sub-operators

6.1 The Customer authorises FirstNet to engage the Sub-operators shown on the Sub-operator List (Annex B), and the Vendors named in the Service Specific Terms, for the Services the Customer orders.

6.2 FirstNet will impose on each Sub-operator, in a written agreement, data protection obligations that give at least the protection required by sections 19 to 21 of POPIA. Where the Sub-operator is a Vendor that offers only its standard terms (for example a global cloud platform), FirstNet will rely on the Vendor's published data processing terms, which are identified in the Service Specific Terms or provided with the Service Schedule.

6.3 FirstNet will give at least 30 (thirty) calendar days' notice of a new Sub-operator, or a change in the country where a Sub-operator processes Customer Personal Information, by updating the Sub-operator List and notifying the Customer in writing.

6.4 The Customer may object to a new Sub-operator on reasonable data protection grounds by written notice within that 30-day period. FirstNet will then try in good faith to offer an alternative. If it cannot, the Customer may end the affected Service on written notice without an early termination charge, except for Vendor commitments under clause 19.4 of the Standard Terms and Conditions.

6.5 FirstNet remains responsible to the Customer for its Sub-operators' processing of Customer Personal Information, subject to clause 5 (Vendor services) and clause 16 (limitation of liability) of the Standard Terms and Conditions.

6.6 In an emergency (for example to restore a Service after an outage or security incident), FirstNet may engage a replacement Sub-operator immediately and will notify the Customer as soon as reasonably possible afterwards.

7. Location of processing and cross-border transfers (POPIA section 72)

7.1 South Africa by default. FirstNet stores and processes Customer Personal Information in South Africa, unless (a) the Service Schedule names a site outside South Africa, or (b) the Service uses a Vendor cloud platform that processes data outside South Africa, as stated in the Service Specific Terms or the Sub-operator List. In either case clause 7.3 applies.

7.2 Where a Service involves processing outside South Africa, the Service Specific Terms will state the country or region. By ordering that Service the Customer instructs FirstNet to make that transfer.

7.3 FirstNet will transfer Customer Personal Information outside South Africa only where one of the conditions in section 72(1) of POPIA is met, namely where:

- 7.3.1 the recipient is subject to a law, binding corporate rules or a binding agreement that provides an adequate level of protection substantially similar to POPIA's conditions for lawful processing, including rules on onward transfer (section 72(1)(a)); or
- 7.3.2 the data subject has consented (section 72(1)(b)), where the Customer has confirmed that it has obtained that consent; or
- 7.3.3 the transfer is necessary for the performance of a contract with the data subject or in the data subject's interest under section 72(1)(c) to (e).

7.4 FirstNet will normally rely on clause 7.3.1, through its agreements with Sub-operators or the Vendor's data processing terms (for example standard contractual clauses or equivalent commitments). FirstNet will give the Customer a summary of the relevant terms on request.

7.5 Where a Service offers a choice of data location (such as a South African or other region), the Customer is responsible for the choice it makes, and FirstNet will not change the location without the Customer's instruction or notice under clause 6.3.

8. Security Compromises (POPIA sections 21(2) and 22)

8.1 FirstNet will notify the Customer immediately, and in any event without undue delay, after becoming aware of a Security Compromise affecting Customer Personal Information, as required by section 21(2) of POPIA.

8.2 The notice will include, as far as is then known: the nature of the Security Compromise; the categories and approximate number of data subjects and records affected; the likely consequences; the measures taken or proposed to address it and reduce its effects; and a contact person at FirstNet. FirstNet will give further information as it becomes available.

8.3 FirstNet will take reasonable steps to contain the Security Compromise, restore the integrity of the affected systems and prevent a recurrence, and will co-operate with the Customer's investigation.

8.4 As responsible party, the Customer decides whether and how to notify the Information Regulator and affected data subjects under section 22 of POPIA. FirstNet will provide the information and assistance the Customer reasonably needs to do so. FirstNet will not notify the Customer's data subjects or the Information Regulator about a Security Compromise affecting Customer Personal Information without the Customer's agreement, unless the law requires it.

8.5 Notification by FirstNet is not an admission of fault or liability.

8.6 The Customer must notify FirstNet promptly of any Security Compromise it becomes aware of that involves a Service, including compromised credentials.

9. Data subject requests and assistance

9.1 If FirstNet receives a request from a data subject to access, correct, delete or object to the processing of Customer Personal Information, it will refer the data subject to the Customer (where it can identify the Customer) and will not respond itself, unless the law requires it.

9.2 FirstNet will give the Customer reasonable assistance, taking into account the nature of the Service and the information available to FirstNet, to respond to data subject requests, to conduct personal information impact assessments, to apply for prior authorisation under section 57 of POPIA where required, and to respond to the Information Regulator.

9.3 Many Services allow the Customer to access, correct, export and delete Customer Personal Information itself. Where they do not, or where the assistance takes significant effort, FirstNet may charge for it at its standard rates, agreed with the Customer in advance.

10. Audits and information

10.1 FirstNet will make available to the Customer the information reasonably necessary to show that it complies with this Annexure, which will normally be its current ISO/IEC 27001:2022 certificate and statement of applicability summary, answers to a reasonable security questionnaire once a year, and relevant Vendor certifications or reports.

10.2 If that information is not enough to show compliance, or the Information Regulator requires it, or a Security Compromise has occurred, the Customer (or an independent auditor bound by confidentiality and not a competitor of FirstNet) may audit FirstNet's compliance with this Annexure:

10.2.1 on at least 30 (thirty) calendar days' written notice (or shorter notice after a Security Compromise);

10.2.2 not more than once in any 12 (twelve) month period, except after a Security Compromise or if required by a regulator;

10.2.3 during Business Hours, without unreasonable disruption to FirstNet's operations, and without access to other customers' data or to information that would compromise FirstNet's security; and

10.2.4 at the Customer's cost, including FirstNet's reasonable costs for the staff time the audit requires.

10.3 Audits of Sub-operators are limited to the audit reports and certifications they make available, unless the Sub-operator's terms allow more.

10.4 Access to FirstNet's data centres for audits is subject to FirstNet's data centre access rules.

11. Return and deletion

11.1 When a Service ends, FirstNet will make Customer Data processed in that Service available to the Customer for retrieval for the period stated in the Service Specific Terms or Service Schedule (or, if none is stated, for a reasonable period that FirstNet confirms to the Customer in writing) after the Termination Date, in the format and by the method set out in the Service Specific Terms (or, if none is stated, in a commonly used format agreed with the Customer at the Customer's cost).

11.2 After that period, FirstNet will delete or de-identify Customer Personal Information in that Service within a reasonable time, including in backups as they expire in their normal rotation, unless the law requires FirstNet to keep it. Where FirstNet must keep information, clause 4 continues to apply and FirstNet will process it only for the purpose for which it must be kept.

11.3 FirstNet will confirm deletion in writing on request.

11.4 Retention of communication-related information required by RICA is not affected by this clause 11.

12. Special personal information and children

12.1 The Customer must tell FirstNet before it uses a Service to process special personal information (such as health, biometric, religious, criminal or trade union information) or personal information of children in large volumes, so that FirstNet can confirm that the Service and its security measures are appropriate.

12.2 Some Services are not designed for those categories of information. The Service Specific Terms will say so.

13. Liability

13.1 Each Party's liability under this Annexure is subject to clause 16 (limitation of liability) of the Standard Terms and Conditions, or the corresponding clause of the Customer's Master Services Agreement.

13.2 Each Party is responsible for administrative fines imposed on it under POPIA as a result of its own conduct.

14. Term

14.1 This Annexure applies for as long as FirstNet processes Customer Personal Information, including after the Agreement ends until deletion under clause 11.

Annex A: Description of processing

Item	Description
Subject matter	Provision of the Services ordered under the Service Schedule.
Duration	The term of the relevant Service plus the retrieval and deletion periods in clause 11.
Nature and purpose	Hosting, storage, backup, replication, transmission, routing, filtering, monitoring, recording, analysis and support, as needed to provide each Service.
Categories of data subjects	Determined by the Customer: typically its employees, contractors, customers, suppliers, website users, callers, guests and other individuals whose information the Customer stores in or transmits through the Services.
Categories of personal information	Determined by the Customer: typically names, contact details, identifiers, user credentials, communications content (email, voice, messages, call recordings), traffic and usage records, files and documents, device and network identifiers, and Inputs and Output of AI Services.
Special personal information	Only if the Customer chooses to process it, subject to clause 12.
Location	South Africa, unless the Service Specific Terms, Service Schedule or Sub-operator List state otherwise.
Sub-operators	As shown on the Sub-operator List (Annex B).

Service-specific details:

Service type	Typical processing by FirstNet as operator
Connectivity (fibre, broadband, LTE/5G, SD-WAN, LEO satellite)	Transmission of traffic; routing and traffic management; logs of IP assignment and usage. Records FirstNet must keep by law (including under RICA) are processed by FirstNet as a responsible party (clause 1.2). FirstNet does not inspect traffic content except for security, filtering or traffic management functions the Customer orders, or as required by law.
Managed Guest Wi-Fi	Guest login and consent records, contact details provided by guests, device identifiers and visit analytics, processed for the venue (the Customer), which is the responsible party, on the Vendor platform named in the Service Specific Terms.

Service type	Typical processing by FirstNet as operator
Cloud, hosting, colocation, backup and disaster recovery	Storage and processing of Customer Data in FirstNet or Vendor infrastructure. In colocation, FirstNet does not access the Customer's equipment or data, except as instructed by the Customer (for example for remote hands).
Security (firewall, SASE, EDR or MDR, email security)	Inspection of traffic, email and endpoint telemetry to detect and respond to threats; security logs; incident investigation.
Voice (cloud PBX, Teams calling, contact centre, call recording)	Call routing on the Customer's configuration; voicemail; call recordings and transcripts where the Customer enables them. FirstNet processes call detail records and other communication-related information it must keep by law as a responsible party (clause 1.2).
Sovereign AI (FirstCoreAI)	Processing of Inputs and generation of Output on the AI Factory; transient caching; logs as described in the Service Specific Terms. Not used for training under clause 26.4 of the Standard Terms and Conditions.
Managed and support services	Access to Customer systems and data to perform support, monitoring and administration tasks.

Annex B: Sub-operator List

This list shows the Sub-operators FirstNet uses for each type of Service. A Sub-operator processes Customer Personal Information only for the Services the Customer orders. Where a location is outside South Africa, the transfer is made under clause 7.3. "To be confirmed" means FirstNet has not yet confirmed the location; until it does, the Vendor processes data in the locations it publishes for its service and, where this is outside South Africa, FirstNet relies on section 72 of POPIA as set out in the Service Specific Terms.

Sub-operator	Services	What it processes	Location	Transfer basis
Mimecast	Email Security (Mimecast)	Email content and metadata, archives and user details	South Africa. Mimecast support and some threat-intelligence functions may process data elsewhere	POPIA s72(1)(a) (Mimecast data processing terms) for any processing outside South Africa
Druva	Microsoft 365 and endpoint backup (Druva)	Backup copies of Customer Data	South Africa (Storage Region). Druva affiliates and its hosting sub-processors may access data from outside South Africa for support and operations	POPIA s72(1)(a) (Druva Data Processing Addendum) for that access
Netskope	Security Service Edge; SD-WAN	User traffic, tenant logs and event data	South Africa (tenant). Traffic of users outside South Africa is processed at the nearest Netskope data centre	POPIA s72(1)(a) (Netskope data processing terms) for traffic processed outside South Africa
CallCabinet	Compliance Call Recording	Call recordings and call metadata	South Africa	None needed, unless the Service Schedule names another region (then POPIA s72)
Smarsh	Compliance Call Recording	Call and message recordings and metadata	South Africa	None needed, unless the Service Schedule names another region (then POPIA s72)

Sub-operator	Services	What it processes	Location	Transfer basis
Purple	Managed Guest Wi-Fi	Guest login and consent records, contact details, device identifiers and visit analytics	South Africa. Some Purple subprocessors (for example email delivery and support) and OTP messaging providers may be outside South Africa	POPIA s72(1)(a) (Purple data processing terms) for those subprocessors
Yeastar (core PBX)	Managed Cloud PBX	Call routing, extensions, voicemail and call recordings	South Africa	None needed
Yeastar (AI Modules) and the AI services Yeastar engages	Managed Cloud PBX (AI Receptionist, AI Transcription)	Call audio and transcripts	To be confirmed	POPIA s72 if outside South Africa
Sophos (Sophos Central, Sophos MDR, Sophos Email)	Managed Detection and Response; Managed Firewall (Sophos); Email Security (Sophos Email); SD-WAN	Endpoint and security telemetry, security logs, email content and firewall management data	Ireland or Germany (region chosen at setup; the Customer may choose)	POPIA s72(1)(a) (Sophos data processing addendum)
Fortinet (FortiEDR cloud)	Managed Detection and Response, where the Service Schedule includes FortiEDR	Endpoint telemetry and security events	European Union	POPIA s72(1)(a) (Fortinet data processing addendum)
Fortinet (FortiGuard and FortiCare)	Managed Firewall (Fortinet)	Device registration, licensing, support and threat-intelligence queries	To be confirmed	POPIA s72 if outside South Africa
Veeam (Veeam Data Cloud Vault, on Microsoft Azure or Amazon Web Services infrastructure)	Backup as a Service	Backup data	South Africa (Veeam's South African region). EU region only for the long-term archive tier, if the Customer asks for it. Veeam support may access Vault metadata from outside South Africa	POPIA s72(1)(a) (Veeam Data Processing Addendum) for the EU archive tier and support access
iOnline	Mobile Data (Private APN portal)	Portal users' usernames and email addresses	South Africa	None needed
Teraco	Colocation at Teraco Sites	Visitor identity details for site access. Teraco houses equipment but does not access Customer Data	South Africa	None needed
Microsoft	Microsoft Cloud (CSP); Microsoft Teams Calling; Microsoft 365 Security	Tenant data, Teams call content, call records and voicemail. Microsoft processes Tenant data under its own agreement with the Customer (Microsoft CSP SST 8.1)	The locations Microsoft publishes for each service	POPIA s72 under the Customer's agreement with Microsoft
Cloudflare	Cloudflare Services; SD-WAN	Traffic, configuration, analytics and logs	To be confirmed	POPIA s72(1)(a) (Cloudflare Data Processing Addendum)

Sub-operator	Services	What it processes	Location	Transfer basis
Zoom	Zoom Phone and Contact Centre	Call content, recordings, transcripts, contact-centre interactions and AI Companion data	To be confirmed	POPIA s72 (Zoom data processing addendum)
Truecaller	Verified Business Caller ID	Brand profile data, call reasons and numbers called	To be confirmed	POPIA s72 (FirstNet's agreement with Truecaller)
Smartz	Smartz Contact Centre	Contact-centre Customer Data	To be confirmed	POPIA s72 if outside South Africa
Apex BI	Call Analytics (Clarity)	Call Data (employee names, extensions, call activity and numbers called)	To be confirmed	POPIA s72 (Apex BI data processing terms)
Sendmarc	Managed DMARC	DMARC report data	To be confirmed	POPIA s72 if outside South Africa
Peplink (InControl 2, SpeedFusion Cloud)	Bonded Connectivity (Peplink)	Device and link data, client device identifiers, GPS location and usage data	To be confirmed	POPIA s72 (Peplink Terms)
Eutelsat OneWeb, its Distribution Partner, and Starlink (Sites outside South Africa only)	LEO Satellite	Customer traffic carried through satellite ground stations	To be confirmed	POPIA s72 (their data protection terms)
GoDaddy, Marcaria and other gTLD and foreign ccTLD Registrars and Registries	Domain Services	Registrant and contact details	Outside South Africa (GoDaddy and Marcaria are based in the United States); other locations to be confirmed	POPIA s72(1)(c) or (d) (needed to perform the contract)
Last-Mile Operators and Network Operators named in the Service Schedule	Dedicated Internet Access; Business Broadband; Mobile Data	Site and contact details for installation and repair; SIM traffic	To be confirmed	POPIA s72 if outside South Africa

Annex C: Summary of security measures

C1. Governance: information security policies approved by management; a named information security owner; risk assessments; supplier security reviews; ISMS certified to ISO/IEC 27001:2022 by INTERCERT (certificate IC-IS-2512139), with annual surveillance audits.

C2. People: background screening where lawful; confidentiality undertakings; security and privacy awareness training; disciplinary process for breaches.

C3. Access control: role-based access on a least-privilege basis; multi-factor authentication for administrative access; prompt removal of access when roles change; periodic access reviews.

C4. Physical security: access-controlled data centres with logged and pre-authorised access, CCTV, and visitor escorting, as described in FirstNet's data centre access rules; colocation in third-party facilities that hold their own certifications (Teraco, for example, holds its own ISO/IEC 27001 certificate for its facilities).

C5. Technical measures: network segmentation and firewalling; encryption in transit for management and customer-facing interfaces; encryption at rest where the Service provides it; vulnerability management and patching; logging and monitoring; malware protection; secure configuration baselines.

C6. Resilience: backups and redundancy appropriate to each Service as described in the Service Specific Terms; business continuity and disaster recovery plans that are tested.

C7. Incident management: a documented incident response process, including the notification steps in clause 8.

C8. Secure disposal: secure deletion of data and destruction of storage media at end of life.

Data Processing Annexure | Version v2026.11a | Effective date: 1 November 2026

Published by FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07), 26 Augrabies Road, Waterfall Office Park, Midrand, 1686 | 0861 989 896 | support@firstnet.co.za

Published by FirstNet Technology Services (Pty) Ltd, registration number 2006/031608/07. Data Processing Annexure, v2026.11a. The current version of every FirstNet legal document is at www.firstnet.co.za/legal-notices/.