Data Processing Agreement

Background

The processor (Telgea) is a mobile plan provider that will provide `{company_name}` with mobile plans. The Processor will process certain personal data on behalf of the Company when performing the services under the Service Agreement.

The Company solely determines the purposes and means of the processing of the Personal Data, and is thus the controller. This DPA governs the Processor's processing of Personal Data on behalf of the Company. In case of conflict between the Service Agreement and this DPA, this DPA shall take precedence to the extent it provides better protection for the Personal Data.

Definitions

The terms defined in Regulation (EU) 2016/679 ("GDPR") shall have the same meaning in this DPA, unless otherwise expressly stated. "Data Protection Law" means applicable data protection legislation, including the GDPR and applicable national data protection legislation.

Processing Data

The Processor shall process Personal Data solely for the purposes instructed by the Company, in accordance with applicable Data Protection Law and this DPA. The Processor shall promptly notify the Company if it cannot comply with this DPA or if an instruction conflicts with Data Protection Law. Any requested deletion shall be completed within twelve (12) months. The Processor shall ensure only authorized personnel with a need-to-know access process Personal Data.

Security

The Processor will take appropriate technical and organizational measures to ensure a level of security appropriate to the risk in accordance with Article 32 of the GDPR, including:

a) Pseudonymization and encryption of Personal Data (where appropriate);

b) Ensuring confidentiality, integrity, availability, and resilience of processing systems;

c) Ability to restore availability and accessibility of Personal Data in a reasonable time;

d) A procedure for regular testing and evaluating the effectiveness of technical and organizational measures.

Personal Data Breaches

The Processor shall notify the Company within 48 hours after becoming aware that a personal data breach has occurred or is imminent. Notification shall contain: a description of the breach; contact details of the Data Protection Officer; likely consequences; and remedial actions taken or proposed.

Sub-processors

The Company consents to the Processor engaging the Sub-Processors listed in Appendix 3. The Processor shall enter into written agreements with each Sub-Processor imposing equivalent data protection obligations. The Processor remains fully liable for the acts and omissions of its Sub-Processors.

Transfer of Personal Data to Third Countries

The Processor shall not transfer Personal Data outside the EU/EEA without the Company's prior written approval, unless based on (i) an adequacy decision, (ii) appropriate safeguards under Article 46 GDPR, or (iii) a derogation under Article 49 GDPR. The Company consents to transfers to the third countries listed in Appendix 4.

Audit and Supervision

The Company is entitled to audit the Processor's compliance with this DPA upon thirty (30) days' prior written notice, during normal business hours, and in a manner that avoids unreasonable disruption. On-site audits are only permitted where information provided is insufficient to verify compliance or where a material security incident has occurred.

Confidentiality

The Processor undertakes not to disclose Personal Data to unauthorized third parties and to ensure all personnel with access maintain confidentiality. If required by law to disclose Personal Data, the Processor shall notify the Company in writing without undue delay.

Damages

Liability arising from the processing of Personal Data under this DPA is subject to the Limitation of Liability provisions set out in the Terms & Conditions, except where mandatory Data Protection Law provides otherwise.

Duration of Agreement

This DPA remains in force for as long as Telgea processes Personal Data on behalf of the Customer under the Agreement.

Miscellaneous

No remuneration is payable under this DPA. Changes to this DPA shall, to be valid, be made in writing and signed by both parties. Neither party may transfer its rights or obligations under this DPA to a third party without the other party's written consent.

Appendix 1 – Scope and Nature of Processing

Category	Details
Categories of Data Subjects	Employees of
Categories of Data Subjects	Employees of {company_name}
Categories of Personal Data	Email, Name, phone number, location data
Purpose of processing	Provide mobile plans to employees
Duration of processing	While using the service
Sub-Processors	YES – see Appendix 3
Transfer to third countries	YES – see Appendix 4

Appendix 2 – Security Measures

1. Data Processing and Hosting

Telgea processes personal data solely for the purpose of providing contracted telecommunications services to its customers, in compliance with the GDPR, UK GDPR, and all applicable data protection laws. All customer data is hosted within the European Union — primary storage in Google Cloud (Europe-West1, Belgium) and Microsoft Azure (West Europe, Netherlands), both ISO 27001 and SOC 2 Type II certified. No personal data is stored outside the EU/EEA. All data at rest and in transit is encrypted using AES-256 and TLS v1.2 or higher. Redundant infrastructure ensures 99% availability with RPO/RTO targets under four (4) hours.

2. Technical and Organizational Measures (TOMs)

Technical controls include: Encryption and pseudonymization of all personal data; Firewalls, intrusion detection and prevention systems, and continuous network monitoring; Strict role-based access controls and least-privilege principles; Periodic internal and external security audits.

Organizational controls include: Personnel subject to signed confidentiality and data protection undertakings; Mandatory data protection and security training; Alignment with ISO 27001, ISO 27701, and SOC 2 Type II.

3. Authentication and Access Management

Access to Telgea systems is restricted to authorized personnel only, managed through SSO, MFA, and 2FA. All access activities are logged and monitored.

4. Data Retention and Deletion

Customer account data is retained for the duration of the agreement plus up to twelve (12) months. Telecommunications records are retained for up to five (5) years, or longer if required by applicable telecom legislation. At the end of the retention period, data is securely deleted or anonymized.

5. Breach Notification and Incident Response

In the event of a personal data breach, Telgea shall notify the affected customer and, where applicable, the relevant supervisory authority within forty-eight (48) hours. Notifications include the nature of the breach, likely consequences, and remedial actions. Telgea has experienced no reportable data breaches within the past two years.

6. Compliance, Audits, and Certification

Telgea's operations comply with GDPR, UK GDPR, applicable national telecom regulations, and the European Electronic Communications Code (EECC). Security controls are aligned with ISO 27001, ISO 27701, SOC 2 Type II, and ISO 42001. Annual internal audits and independent third-party assessments verify compliance.

Appendix 3 – Sub-Processors

SaaS Providers

Processor	Category	Purpose	Customer Data	Residency
Google Cloud EMEA Limited	Cloud hosting	App hosting & storage	All customer data types	EU
Inteserra / JSI	Regulatory	Regulatory filings	Aggregated traffic stats	EU
Google Ireland Limited	Analytics	Docs, files, analytics	Customer contact info	EU
Cloudflare, Inc.	Edge/CDN	Security & performance	IP addresses, metadata	EU
Sentry, Inc.	Monitoring	Errors & performance	Pseudonymous IDs	EU
Better Stack	Logs & uptime	Logs & alerts	IPs, request paths	EU
Google Analytics	Analytics	Website analytics	Device info, cookie IDs	EU
SendGrid	Transactional email	Service emails	Email, name, content	EU
Twilio	SMS/voice	Notifications	Phone numbers, metadata	EU
Stripe	Payments	Payments & fraud detection	Card token, billing info	EU
QuickBooks	Accounting	Invoicing & bookkeeping	Customer billing data	Not EU
Avalara	Tax compliance	VAT/tax automation	Company + billing data	Not EU

Telecom Providers

Processor	Country	Underlying Provider	Purpose	Customer Data	Location
Newsim GmbH	Germany	Telefónica Germany	Local connectivity	Subscriber identifiers, CDR	EU
NetworkIP LLC	USA	Undisclosed	International calling	Phone numbers, call metadata	USA
Telenabler AB	Sweden	Tele 2 AB	Local connectivity	Subscriber profile, SIM, CDR	EU
Telenabler A/S	Denmark	Telenor A/S	Local connectivity	Subscriber identifiers, CDR	EU
Transatel SA	France	Orange S.A.	Local connectivity	Subscriber identifiers, CDR	EU
Transatel Ltd	UK	BT Group plc	Local connectivity	Subscriber identifiers, CDR	EU
MVNOC LLC	USA	Undisclosed	Local connectivity	Subscriber identifiers, CDR	USA
MVNE Sp. Z o.o	Poland	P4 Sp. Z o.o	Local connectivity	Subscriber identifiers	EU
Tata Ltd	Netherlands	KPN N.V.	Local connectivity	Subscriber identifiers	EU

Appendix 4 – Third Countries for Data Transfers

Telgea applies the following safeguards for international transfers of data:

Contractual: Standard Contractual Clauses (SCCs) issued by the European Commission.

Transfer Impact Assessment: Telgea evaluates privacy and surveillance laws in the recipient country, the risk of access by public authorities, and the effectiveness of additional safeguards.

Technical Safeguards: All data transfers use strong encryption; data is encrypted at rest and in transit with keys managed within the EEA.

Organizational Safeguards: Data minimization; access limitation; mandatory confidentiality agreements for all employees and subprocessors; regular security and privacy training.