Annex B – Privacy & POPIA Processing Notice

Attached to the Digissential Master Legal Policies & Terms (South Africa)

Effective date: 2025-08-13

1. Purpose & Scope

1.1 This Annex sets out Digissential's privacy governance and personal information processing practices in terms of the Protection of Personal Information Act 4 of 2013 ("POPIA") and related regulations. It applies to all Services and to all Personal Information processed by Digissential (the "Company") as a Responsible Party and, where applicable, as an Operator.

1.2 This Annex should be read with the Master Legal Policies & Terms (Data Handling, Confidentiality, Remote Services, Security, Jurisdictional Compliance). Where there is any ambiguity, the stricter protection for data subjects shall prevail.

1.3 This Annex also supports compliance with the Promotion of Access to Information Act 2 of 2000 ("PAIA"). The Company will maintain a PAIA Manual and make it available on request or via its official channels.

2. Roles, Governance & Contact

2.1 Responsible Party: Digissential ("the Company").

2.2 Information Officer: The head of the private body (as defined in POPIA and PAIA) is designated as the Information Officer and registered with the Information Regulator. Contact: digissentialteam@gmail.com.

2.3 Operators (Processors): Reputable third-party service providers may be engaged for cloud storage, email, payments, diagnostics tooling and communications. Operators process Personal Information only on documented instructions, under written agreements meeting POPIA sections 19–21, including prompt breach notifications to the Company.

2.4 Supervisory Authority: Information Regulator (South Africa). Complaints may be lodged with the Regulator or raised with the Company first for internal resolution.

3. Definitions

3.1 "Personal Information" has the meaning in POPIA and includes any information relating to an identifiable, living, natural person, and where applicable an identifiable, existing juristic person.

3.2 “Special Personal Information” includes, inter alia, religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information and criminal behaviour, as defined in POPIA.

3.3 “Processing” means any operation concerning Personal Information, including collection, receipt, recording, organisation, storage, updating, retrieval, dissemination, and destruction.

3.4 “Confidential Information” means non-public technical, business, device or customer information disclosed in connection with the Services, including photographs, configurations, logs and credentials.

3.5 “Information Officer” means the individual designated in terms of POPIA responsible for compliance, internal monitoring, training, and liaison with the Information Regulator.

3.6 “Unique Identifier” includes a South African ID number or other assigned identifier used for uniquely identifying a data subject.

4. Lawful Processing Conditions & Notification

4.1 The Company processes Personal Information in accordance with POPIA’s conditions of lawful processing: accountability; processing limitation (lawfulness, minimality, consent or other lawful ground); purpose specification; further processing limitation; information quality; openness; security safeguards; and data subject participation.

4.2 Lawful grounds for processing include one or more of the following as applicable:

- 4.2.1 Consent of the data subject (ECTA-valid electronic consent permitted).
- 4.2.2 Processing necessary to conclude or perform a contract with the data subject.
- 4.2.3 Processing required by law (e.g., tax, accounting, second-hand goods records).
- 4.2.4 Processing to protect the legitimate interests of the data subject.
- 4.2.5 Processing necessary for pursuing the legitimate interests of the Company or a third party, balanced against data subject rights.

4.3 Notification at collection (POPIA s18): The Company provides data subjects with the required information at or before collection (e.g., via intake forms and this Annex), including the identity of the Company, the purpose of collection, whether supply is voluntary or mandatory and consequences of failure, any law authorising collection, recipients or categories of recipients, the nature or source of the information (where not obtained from the subject), and data subject rights (including the right to lodge a complaint with the Information Regulator).

5. Categories of Personal Information Processed

- 5.1 Identification & Contact: name, email, phone, address.

- 5.2 Device & Service Data: device identifiers/serials, specifications, service logs, error reports, configuration details, photographs of device condition.
- 5.3 Transaction & Billing: quotes, invoices, payments, proof of payment, VAT details where applicable.
- 5.4 Communications: emails, messages, call notes, remote session metadata (timestamps, session IDs).
- 5.5 Verification: limited ID checks where required for password resets or fraud prevention (Unique Identifiers processed only when strictly necessary and not used for unrelated linkage or profiling).
- 5.6 Special Personal Information: not intentionally collected. Any incidental exposure is not accessed or processed beyond what is strictly necessary to perform Services or comply with law, with suitable safeguards.

6. Purposes of Processing

- 6.1 Service delivery: diagnostics, repair, configuration, remote support, custom builds.
- 6.2 Client management: intake, scheduling, job tracking, communications and handover.
- 6.3 Billing & accounting: invoicing, receipts, tax compliance and audit trail.
- 6.4 Security & fraud prevention: verification where appropriate, incident response and investigation.
- 6.5 Quality control & training: limited review of logs/records to improve Services.
- 6.6 Legal obligations: compliance with POPIA, CPA, tax law and second-hand goods record-keeping.

7. Special Personal Information & Children

7.1 The Company does not intentionally collect Special Personal Information. If processing becomes necessary, it will rely on an applicable POPIA ground (including explicit consent, exercise/defence of a right, or other statutory basis), apply heightened safeguards and document the justification.

7.2 The Services are not directed at children. The Company does not knowingly process children's Personal Information without lawful justification and, where required, verified consent of a competent person.

8. Security Safeguards

- 8.1 Access controls: least-privilege roles; approval for elevated access; regular access reviews.
- 8.2 Storage: secure cloud storage with encryption in transit and at rest (where available); minimal local storage with device encryption and strong authentication.
- 8.3 MFA: multi-factor authentication on core accounts where supported.
- 8.4 Operational security: secure password handling, patching, malware protection and secure disposal of media.

- 8.5 Physical security: secured workspace; locked storage for devices and parts; visitor controls where applicable.
- 8.6 Operator management: written operator contracts requiring POPIA-level safeguards and immediate breach notification to the Company.
- 8.7 Data minimisation & information quality: collect only what is necessary; take reasonably practicable steps to ensure information is complete, accurate and updated when necessary.

9. Cross-Border Transfers (POPIA s72)

9.1 Personal Information may be transferred to or stored in jurisdictions outside South Africa (e.g., reputable cloud providers). Transfers will occur only where:

- 9.1.1 The recipient is subject to a law, binding corporate rules, or binding agreement providing an adequate level of protection; or
- 9.1.2 The data subject consents; or
- 9.1.3 The transfer is necessary for performance of a contract or for the benefit of the data subject; or
- 9.1.4 It is not reasonably practicable to obtain consent, but consent would likely be given, and the transfer is for the benefit of the data subject.

10. Direct Marketing (POPIA s69)

10.1 Electronic direct marketing to new prospects is conducted only with prior, express consent in accordance with POPIA and its regulations. Existing clients may receive marketing about similar products/services, with a functional, no-cost opt-out included in each message.

10.2 Consent records and suppression lists are maintained to honour opt-out choices.

11. Retention & Destruction

- 11.1 Service records, photographs and diagnostic logs: retained for three (3) years unless longer retention is required for legal claims or warranty.
- 11.2 Financial records (invoices, payments): retained for at least five (5) years to meet tax and accounting obligations.
- 11.3 Remote session logs: retained for up to thirty (30) days unless required longer for security or legal reasons.
- 11.4 Security incident records: retained for at least three (3) years or longer where required by law.
- 11.5 On expiry of the retention period, data is securely destroyed or irreversibly anonymised.

12. Data Subject Rights & Requests

12.1 Data subjects may request access to, correction or deletion of their Personal Information, object to processing, or withdraw consent (where consent is the basis). Requests must include sufficient identification for verification.

12.2 The Company will respond within a reasonable time, not exceeding thirty (30) days, unless an extension is permitted by law. Certain requests may be declined where a lawful ground applies (e.g., to protect third-party rights or where records must be retained by law). Requests relating to access may be processed in terms of PAIA procedures.

12.3 The Company does not make decisions based solely on automated processing that produce legal or similarly significant effects on data subjects.

13. Prior Authorisation (POPIA s57–s58)

13.1 The Company does not presently engage in processing operations requiring prior authorisation by the Information Regulator. Should such processing be proposed (e.g., processing of Unique Identifiers for unrelated linkage or certain categories of Special Personal Information), the Company will obtain the Regulator's authorisation prior to commencement.

14. Security Compromises & Breach Notification (POPIA s22)

14.1 In the event of a security compromise, the Company will notify the Information Regulator and affected data subjects as soon as reasonably possible after becoming aware, describing the nature of the compromise, possible consequences, measures taken or proposed, and recommendations for the data subject.

14.2 Notifications may occur via email, website notice, public communication, or other method directed by the Regulator, taking account of practicality and security. Operators are obligated by contract to notify the Company immediately upon becoming aware of a compromise.

15. Openness & Documentation

15.1 The Company maintains internal documentation of processing activities, operator agreements and security measures, available to the Information Regulator upon lawful request.

16. Updates & Versioning

16.1 This Annex may be updated to reflect changes in law, guidance by the Information Regulator, or the Company's practices. Material changes will be signposted on official channels. The Master Legal Policies & Terms control in the event of conflict.

16.2 Version history is recorded in Annex F (Change Log) of the Master Legal Policies & Terms.

17. Queries & Complaints

17.1 Queries and requests must be directed to the Information Officer at digissentialteam@gmail.com. Identification will be required for rights requests.

17.2 Complaints may be lodged with the Information Regulator (South Africa) in accordance with the Regulator's prescribed procedures and forms.