TERMS & CONDITIONS — BoldLine Screening and Vetting

1. Introduction / Parties
1.1 These Terms & Conditions ("Terms") govern the provision of background screening and verification services (the "Services") by BoldLine Screening and Vetting, a company incorporated under the laws of South Africa, registration number 2023/143097/07, having its registered office at 10 Blaauwberg Road, Table View, Cape Town, 7441 ("Provider", "we", "us" or "our"), to the client named in the applicable Service Order ("Client" or "you").
1.2 These Terms apply to background screening services performed in the Republic of South Africa and to any related processing of personal information.

2. Definitions
· Personal Information: as defined in the Protection of Personal Information Act, 2013 ("POPIA").
· Data Subject: the individual (applicant, candidate or employee) whose data is processed for the purposes of a background check.
· PAIA: Promotion of Access to Information Act, 2000.
· NCA: National Credit Act, 2005, where credit reports are requested.

3. Scope of Services
3.1 The Provider offers the Client one or more of the following Services (as ordered): identity verification, criminal record checks (Police Clearance Certificates and SAPS CRC queries), employment history verification, education verification, reference checks, professional license checks, credit checks, social media screening, and other verification services. Use of certain Services (e.g., criminal record or credit checks) is subject to additional legal and procedural requirements described below.

4. Legal Basis & Compliance
4.1 Lawful basis and purpose limitation: The Client represents and warrants that it has a lawful and documented purpose for ordering each background check and that the processing is adequate, relevant and not excessive for that purpose in accordance with POPIA. The Provider will only process Personal Information on the Client's documented instructions and where the Data Subject's consent or another valid legal basis exists.
4.2 POPIA compliance: Both Provider and Client shall comply with POPIA obligations (accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation). The Client acknowledges that the Provider is an operator/processor for the purposes of POPIA and

processes information on the Client's behalf. Each party shall implement appropriate technical and organizational measures to safeguard Personal Information.

4.3 PAIA: The Provider maintains a PAIA manual and will handle PAIA requests in accordance with the Act. Where the Provider is a private body, Client requests for records must be routed through the Provider's PAIA process.

5. Consent & Candidate Notification

5.1 Informed consent: The Client must obtain and retain explicit, written consent from the Data Subject for the background checks ordered, and must provide the Data Subject with the Provider's identity and this contact information. Consent must be specific to the checks to be performed and must include sufficient information to satisfy POPIA's transparency requirements. The Provider will not order checks without evidence of valid consent where required by law.

5.2 Suggested consent clause (sample text — Client must adapt and obtain signatures):

"I hereby consent to [Client] and its appointed screening provider, BoldLine Screening and Vetting, collecting and processing my personal information for the purpose of performing background checks in connection with my application / employment. I understand which checks will be performed (e.g., identity, criminal record, credit, employment, education) and that I may withdraw consent subject to contractual or legal constraints."

6. Types of Checks — Special Requirements

6.1 Criminal record checks / Police Clearance Certificates: Criminal record checks and Police Clearance Certificates must be obtained through SAPS processes when required for a PCC or where formal criminal-history certification is required. Where the Provider uses SAPS or other official sources, the Provider will follow SAPS requirements for fingerprinting, ID documentation and consent. Data Subjects who are foreign nationals may have differing processes.

6.2 Credit checks: Credit checks shall only be requested where lawful and relevant (e.g., positions requiring financial trust), and only where the Client has obtained specific consent in line with the NCA. Credit information will be handled and retained only as permitted by the NCA and applicable credit bureau rules.

6.3 Verification of qualifications, employment and references: Provider will use public records, third-party verifiers, former employers and educational institutions where permitted. Client must ensure the relevance of such checks to the role.

6.4 Special Personal Information: Processing of special personal information (e.g., health, biometric data such as fingerprints) will be done only where the Data Subject has provided explicit consent and where there is a lawful justification. Processing biometric data (e.g., for SAPS fingerprint checks) will be undertaken strictly per law and SAPS/third-party rules.

7. Accuracy, Disputes & Rectification

7.1 Accuracy: The Provider will use reasonable efforts to obtain accurate information, but cannot guarantee the completeness or correctness of third-party records. The Client acknowledges that some public records may be incomplete or outdated.
7.2 Dispute & rectification process: If a Data Subject disputes a result, the Provider will: (a) notify the Client, (b) investigate the dispute with the source,
and (c) correct or annotate records if an error is found. The Provider will inform the Client and the Data Subject of the outcome in accordance with POPIA's data subject participation requirements.

8. Data Retention & Deletion
8.1 Retention periods: Provider will retain Personal Information only for as long as necessary to provide the Services, comply with law, resolve disputes, enforce agreements, and meet record-keeping obligations. Specific data types may require different retention periods (e.g., credit reports may be transient and deleted after compliance windows). For retention related to criminal checks or credit records, Provider will comply with relevant regulations and the Client's documented retention schedule.
8.2 Deletion: On termination of Services or upon documented request where a lawful basis no longer exists, Provider will delete or anonymize Personal Information within a reasonable time frame, subject to legal or contractual retention obligations.

9. Security & Confidentiality
9.1 Provider shall maintain appropriate administrative, technical and physical safeguards to protect Personal Information against loss, unauthorized access, destruction, or disclosure, and will use encryption, access control, logging and secure transmission where appropriate.
9.2 Provider shall promptly notify the Client of any security breach involving Personal Information and assist the Client in satisfying POPIA breach-notification obligations and mitigation measures.

10. Use of Sub-processors and Third Parties
10.1 Provider may engage third parties (including credit bureaux, SAPS or foreign data providers) to perform parts of the Services. Provider will (a) carry out due diligence on sub-processors; (b) contractually bind sub-processors to provide at least the same level of protection required by these Terms and by POPIA; and (c) remain responsible for sub-processor compliance.
10.2 Cross-border transfers: Where Personal Information is transferred out of South Africa, Provider will ensure an adequate level of protection (including contractual safeguards and compliance with POPIA's cross-border transfer requirements).

11. Client Representations & Responsibilities

11.1 The Client warrants that: (a) it has obtained all required consents and has provided clear notices to Data Subjects; (b) the processing requested is lawful, necessary and proportionate; c) it will not request checks that are overly intrusive or unlawful for the role; and (d) it will use the results legally and fairly in hiring/HR decisions, considering rehabilitation and fairness obligations under South African labour law.
11.2 The Client shall indemnify and hold Provider harmless against claims resulting from the Client's failure to obtain valid consent or from Client's unlawful instructions.

12. Fees & Payment
12.1 Fees are set out in the Service Order. The Client agrees to pay invoices within [30] days unless otherwise agreed. Provider may suspend Services for non-payment after providing notice.
13. Limitation of Liability & Warranties
13.1 No absolute warranties: Provider provides Services on a reasonable-efforts basis. Provider does not warrant that third-party data is complete or error-free.

13.2 Limitation of liability: To the maximum extent permitted by law, Provider's aggregate liability for direct damages arising from or in connection with these Terms shall be limited to the fees paid by the Client to Provider for the particular Service in the 12 months preceding the claim. Provider shall not be liable for indirect, special, consequential or punitive damages.
13.3 Nothing in these Terms excludes liability that cannot be excluded under South African law.

14. Data Subject Rights & Complaints
14.1 Data subject rights: Data Subjects may exercise their rights under POPIA (access, correction, deletion, objection, right to withdraw consent). Requests should be made to the Provider's Information Officer at the contact details below. Provider will respond within the time frames required by POPIA.
14.2 Complaints: Data Subjects may lodge complaints with the Information Regulator in addition to Provider's internal complaints procedure. The Provider will cooperate with regulatory investigations.

15. Regulatory Authorisations & Accreditation
15.1 Where certain screening activities require authorisation, licences, or compliance with SAPS or other agency rules (for example, fingerprinting for PCCs), Provider will comply with such rules and ensure documentation of lawful process. Certain background screening service providers may need registration/authorization per guidance from the Information Regulator — Provider confirms it has taken reasonable steps to comply with applicable regulatory guidance.

16. Confidentiality
16.1 Each party shall keep confidential all non-public information received in connection with the Services and shall not disclose such information except as required by law or with the other party's prior written consent.

17. Intellectual Property
17.1 Provider retains all intellectual property rights in the screening methods, reports, software and related materials. Client receives a limited, non-exclusive license to use reports for its internal employment decision-making purposes only.

18. Term, Termination & Survival
18.1 Either party may terminate the Services with 30 days' written notice. Termination will not relieve the Client of outstanding payment obligations. Clauses that by their nature survive termination (e.g., confidentiality, liability limits, data retention obligations) shall survive.
19. Governing Law & Dispute Resolution
19.1 These Terms are governed by the laws of the Republic of South Africa. Parties will attempt to resolve disputes in good faith. If unresolved within 30 days, disputes shall be submitted to the exclusive jurisdiction of South African courts.

20. Amendments
20.1 Provider may amend these Terms for legal, regulatory, or business reasons. Material changes affecting Data Subjects will be notified to Clients and, where required, to Data Subjects.

21. Notices & Contact
21.1 For notices, Data Subject requests or POPIA/PAIA communications:
Information Officer: Thomas Frazer
Email: tomfrazer@boldline.co.za
Postal address: Unit 603, The Aquarius, 10 Blaauwberg Road, Table View, 7441, Cape Town, South Africa
Phone: +27 67 543 3004

22. Miscellaneous
22.1 Entire Agreement: These Terms and the applicable Service Order constitute the entire agreement between Provider and Client with respect to the Services.
22.2 Severability: If any provision is unenforceable, it will be severed and the rest remains in force.

Practical Annexes (suggested to include in final T&C or as separate policies)

Annex A — Sample Candidate Consent Form (short)
"I, [name], ID/Passport [●], consent to [Client] and BoldLine Screening and Vetting processing my personal information for identity verification, criminal record check, employment and education verification, and credit check (if applicable). I understand my rights under POPIA and that I can contact BoldLine Screening and Vetting at +27 67 543 3004. Signature: _____ Date: _____."

Annex B — Retention Schedule (Example)
· Adverse report files: retained for up to 3 years from date of report or as required by Client's HR policies and legal obligations.
· Credit query transient data: deleted within 72 hours after completion unless Client requires retention for bona fide business reasons and has lawful basis.

Annex C — Data Subject Rights & How To Exercise Them
· Step 1: Submit a written request to Information Officer.
· Step 2: Provider acknowledges within 10 business days and provides identity verification steps.
· Step 3: Provider resolves or escalates within statutory timeframes required by POPIA.

Key Legal References (selected)
· Protection of Personal Information Act 4 of 2013 (POPIA).
· Guidance and regulatory resources from the Information Regulator (South Africa).
· SAPS Police Clearance Certificate (PCC) and criminal record procedures.
· National Credit Act requirements for credit checks and consent.
· Practical guidance and commentary on POPIA and background checks from legal and industry sources.