Andeavour

# Technical and Organizational Measures (TOMs)

## Security Measures Addendum - Applicable to Andeavour Offerings

| | |
|---|---|
| **Document owner** | Alliance Andeavour Group Ltd. (Andeavour) |
| **Version** | 1.0 |
| **Effective date** | 15.8.25 |
| **Classification** | Customer Security Documentation |
| **Scope** | Baseline technical and organizational measures applicable to Andeavour Offerings where Andeavour Processes Personal Data on behalf of a Customer. |

## 1. Purpose and Scope

These Technical and Organizational Measures ("TOMs") describe Andeavour's baseline Security Measures for protecting Personal Data processed in connection with Andeavour Offerings. They are intended to operate as the general Security Measures Addendum referenced by Andeavour's standard Data Processing Agreement ("DPA").

These TOMs apply where Andeavour acts as a Processor on behalf of a Customer. The specific nature, scope, duration, categories of Personal Data, deployment model and Customer instructions remain governed by the applicable Agreement and DPA. Additional or more specific controls may be agreed in writing for a particular Offering, deployment or Customer.

## 2. Security and Privacy Principles

- Risk-based security: measures are selected taking into account the nature, scope, context and purposes of Processing and the risks to individuals.
- Data minimization and purpose limitation: Personal Data is processed only as necessary to provide the applicable Andeavour Offering and in accordance with documented Customer instructions.
- Least privilege: access to Personal Data and production systems is limited to authorized personnel and service components that require access for legitimate operational purposes.
- Confidentiality, integrity and availability: controls are designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.
- Privacy by design: security and privacy considerations are incorporated into architecture, configuration, change management and product operations.
- No special-category data under the standard DPA: Customers are expected not to provide Special Categories of Personal Data unless expressly agreed in writing and supported by appropriate safeguards.

# 3. Baseline Technical and Organizational Measures

| CONTROL AREA | BASELINE MEASURE |
|---|---|
| **Security governance** | Andeavour assigns responsibility for security and privacy controls to appropriate technical and management personnel. Security documentation, policies and procedures are maintained and reviewed periodically and upon material changes. |
| **Identity & access management** | Access to production systems, Customer environments and Personal Data is restricted to authorized personnel on a need-to-know basis. Least-privilege principles and authenticated accounts are used for administrative and operational access. |
| **Credential security** | Administrative and service credentials are managed to reduce unauthorized access risk. Access credentials are not intended to be shared between users and are revoked or changed when no longer required. |
| **Confidentiality obligations** | Personnel and contractors with access to Customer information are subject to appropriate confidentiality obligations and internal security/privacy requirements. |
| **Encryption in transit** | Network communications containing Personal Data are protected using encrypted transport protocols where technically applicable. |
| **Encryption at rest** | Personal Data stored in managed cloud or Andeavour-controlled infrastructure is protected using encryption-at-rest capabilities and platform security controls where applicable to the relevant Offering. |
| **Infrastructure security** | Andeavour uses professionally operated infrastructure, including cloud services such as Google Cloud Platform where applicable. Infrastructure access, configuration and service permissions are restricted and managed according to operational need. |
| **Network security** | Network exposure is minimized to required services. Security groups, firewall or equivalent platform controls, restricted service interfaces and secure administrative access are used where applicable. |
| **Data segregation** | Customer data is logically segregated by application, tenant, account, project, environment or equivalent control appropriate to the architecture of the relevant Offering. |
| **Logging & monitoring** | Relevant system, application and security events are logged and monitored as appropriate for operational troubleshooting, detection of anomalous activity and security investigation. Access to logs is restricted to authorized personnel. |

| CONTROL AREA | BASELINE MEASURE |
|---|---|
| **Vulnerability & patch management** | Operating systems, dependencies, libraries, cloud configurations and software components are periodically reviewed. Security updates and material vulnerabilities are prioritized for remediation based on risk and operational impact. |
| **Secure development & change management** | Material changes to production systems are performed by authorized personnel and are tested or reviewed as appropriate. Security and privacy impact are considered for changes that affect data Processing or system exposure. |
| **Data minimization** | Andeavour limits collection and Processing to Personal Data reasonably required to deliver the applicable Offering, support the Customer, satisfy documented instructions or meet legal obligations. Customers are expected to provide only the minimum Personal Data necessary. |
| **Pseudonymization / reduced identifiers** | Where appropriate to the use case and technically feasible, identifiers may be reduced, masked, tokenized, pseudonymized or excluded from downstream processing to limit exposure. |
| **AI-enabled processing** | Where an Offering uses AI models, APIs or agents, Andeavour applies data minimization and access controls to AI inputs and outputs. Approved third-party AI services and Andeavour-controlled models may be used subject to the applicable Agreement, Customer instructions and Sub-processor safeguards. |
| **AI security controls** | Where deployed, Andeavour may use its own security technologies, including AgentGuard, to monitor AI/agent activity, detect anomalous or unauthorized behavior, reduce data-leakage risk and enforce AI usage or governance controls. |
| **Backup & recovery** | Backup and recovery mechanisms are maintained where required for service availability and restoration. Backup scope, frequency and retention are proportionate to the relevant Offering and the data involved. |
| **Availability & resilience** | Andeavour uses infrastructure redundancy, operational monitoring, recovery procedures and other resilience measures appropriate to the relevant service architecture and risk profile. |
| **Security incident response** | Suspected Security Incidents are investigated, contained and remediated as appropriate. Where a Security Incident affects Customer Personal Data, Andeavour notifies the Customer without undue delay in accordance with the DPA and applicable law and provides available information reasonably necessary for the Customer's obligations. |

| CONTROL AREA | BASELINE MEASURE |
|---|---|
| **Retention & deletion** | Personal Data is retained only as needed to provide the applicable Offering, comply with documented Customer instructions, or satisfy applicable business/legal requirements. On termination, Personal Data is deleted or returned as provided by the DPA, subject to lawful retention requirements. |
| **Data Subject Request support** | Andeavour provides reasonable assistance to Customers in responding to Data Subject Requests relating to Personal Data processed through Andeavour Offerings, taking into account the nature of the Processing and the information available to Andeavour. |
| **Sub-processor management** | Sub-processors that may Process Personal Data are engaged under written contractual safeguards appropriate to their role. Andeavour requires applicable data protection obligations and remains responsible for Sub-processor compliance as provided in the DPA. |
| **International transfers** | International transfers of Personal Data are handled using applicable lawful transfer mechanisms and contractual safeguards required by the relevant Data Protection Legislation and DPA. |
| **Government / law-enforcement requests** | If Andeavour receives a legally binding demand for Customer Personal Data, Andeavour follows the process set out in the DPA, including attempting to redirect the request to the Customer and providing notice where legally permitted. |
| **Physical security** | Production infrastructure is generally hosted in professionally managed cloud or data-center environments. Physical security of provider facilities is managed by the applicable infrastructure provider. For Customer-managed or on-premise deployments, applicable physical controls may be the Customer's responsibility. |
| **Review & continuous improvement** | Andeavour periodically reviews the effectiveness and appropriateness of these TOMs and may update controls to address material changes in technology, threat landscape, Processing activities, legal requirements or customer commitments. |

## 4. Technology and Deployment Context

Andeavour Offerings may be delivered through different deployment models depending on the product, Customer requirements and Agreement. The following examples describe common technology contexts and do not require every component to be used for every Customer or Offering.

| COMPONENT / MODEL | PURPOSE | SECURITY / DATA HANDLING |
|---|---|---|

| | | |
|---|---|---|
| **Professional cloud infrastructure (including GCP where applicable)** | Hosting, compute, storage, networking, security and logging. | Customer data is protected using relevant platform controls, restricted permissions, encryption capabilities and environment configuration appropriate to the Offering. |
| **Approved AI model/API providers (including Google Gemini where applicable)** | AI-assisted analysis, search, inference, classification, monitoring or other Offering functions. | Only information required for the relevant task is provided, subject to Customer instructions, contractual safeguards and applicable Sub-processor controls. |
| **Andeavour-controlled AI models and GPU infrastructure** | Internal model execution, inference and product-specific AI processing. | Access is restricted to authorized service components and personnel; processing is subject to the same baseline access, logging, retention and security controls described in these TOMs. |
| **Andeavour security technologies (including AgentGuard where deployed)** | AI security, governance, anomaly monitoring and data-leakage risk reduction. | Security telemetry and controls are applied as appropriate to the relevant architecture and customer configuration. |
| **Customer-managed / on-premise deployment where supported** | Deployment within Customer infrastructure or an agreed dedicated environment. | Responsibility for certain infrastructure, physical, identity, network, backup or operational controls may be allocated to the Customer as specified in the Agreement or implementation documentation. |

## 5. Customer Responsibilities and Shared Security

Security is a shared responsibility. Customers are responsible for lawful collection and disclosure of Personal Data provided to Andeavour, maintaining an appropriate legal basis and notices, minimizing Personal Data, protecting Customer-managed credentials and devices, and configuring Customer-controlled systems in accordance with the Agreement and DPA.

Where a deployment places infrastructure or security controls under Customer administration, the Customer is responsible for those controls to the extent described in the applicable Agreement, implementation documentation or shared-responsibility model.

## 6. Maintenance and Applicability

These TOMs are the general baseline applicable to Andeavour Offerings as of the effective date above. They may be supplemented by product-specific security documentation, implementation guides, a Sub-processor list, customer-specific addenda, or other Security Documentation. In the event of a conflict, the applicable Agreement, DPA and mandatory Data Protection Legislation govern according to their stated order of precedence.

Andeavour may update these TOMs to reflect improvements, infrastructure changes, legal requirements or the threat environment, provided such updates do not materially reduce the overall protection of Personal Data during an active contractual term unless otherwise agreed.