Trust & Security Overview

This Trust & Security Overview describes the Company’s approach to security, reliability, data protection, and operational trust practices in connection with the Platform. This document is provided for informational and transparency purposes only and does not form part of the contractual agreement between the Company and the Customer, unless expressly incorporated by reference. This document does not constitute any representation, warranty, or commitment regarding the performance, availability, or security of the Platform.

This document is intended to support Customer due diligence, internal risk assessments, and IT or procurement reviews.

---

1. Purpose and Scope

The Company is designed to maintain the security, integrity, and availability of the Platform in a commercially reasonable manner. This Trust & Security Overview outlines the principles, controls, and practices implemented to support secure operation of the Platform.

This document applies to the Platform’s standard production environment and does not apply to beta features, experimental services, or customer-specific customizations unless otherwise agreed.

---

2. Shared Responsibility Model

Security and compliance are shared responsibilities between the Company and the Customer.

The Company is responsible for securing the Platform infrastructure, systems, and services it operates. Customer is responsible for securing its own systems, user access, configurations, and Campaign content, as well as ensuring lawful use of the Platform.

---

3. Platform Architecture and Infrastructure

The Platform is hosted using reputable cloud infrastructure providers and is designed with scalability, redundancy, and fault tolerance in mind.

The Company employs standard architectural practices intended to mitigate risks associated with single points of failure and support reliable operation. Specific infrastructure details are not disclosed for security reasons.

---

4. Access Controls and Authentication

Access to the Platform is restricted to authorized users through role-based access controls.

Administrative access is limited to authorized personnel and governed by internal access policies. Authentication mechanisms are designed to mitigate the risk of unauthorized access.

Customer is responsible for managing user permissions and protecting account credentials.

---

5. Data Protection and Encryption

The Company implements reasonable technical measures designed to mitigate risks to data processed through the Platform.

Data in transit is protected using industry-standard encryption protocols. Data at rest may be encrypted depending on system design and risk considerations.

The Company does not guarantee absolute security and recognizes that no system can be fully secure.

---

6. Monitoring and Logging

The Company maintains monitoring and logging practices designed to detect abnormal system behaviour, performance degradation, and potential security events.

Logs may be used for operational troubleshooting, security analysis, and service improvement purposes and are retained in accordance with internal policies.

---

7. Vulnerability Management

The Company employs reasonable practices to identify and address security vulnerabilities, which may include internal testing, updates, and patching activities.

The Company does not commit to specific remediation timelines and prioritizes vulnerabilities based on risk and impact.

---

8. Incident Response

The Company maintains internal incident response procedures intended to identify, assess, and respond to security incidents.

In the event of a material security incident affecting Customer data, the Company will use reasonable efforts to notify Customer within a commercially reasonable timeframe after becoming aware of such incident.

---

9. Data Retention and Deletion

Campaign-related data is retained for a limited period following Campaign expiration in accordance with the Company's data retention practices.

Retention periods and deletion practices may vary based on service configuration and may be updated from time to time. In certain cases, data may be retained in backups or system logs for operational or security purposes and is removed in the ordinary course of system operations.

---

10. Sub-Processors and Third-Party Services

The Company may engage third-party service providers to support Platform operations, including infrastructure hosting, monitoring, and communications services.

The Company selects service providers using commercially reasonable diligence and oversees their engagement in accordance with internal policies.

---

11. Compliance and Certifications

The Platform is designed to support Customer compliance efforts; however, the Company does not represent or warrant compliance with any specific regulatory framework or certification unless expressly stated.

Customers remain responsible for determining whether the Platform is suitable for their regulatory and compliance requirements.

12. Customer Due Diligence

The Company may provide reasonable high-level information regarding its security and trust practices in response to Customer due diligence inquiries.

The Company is not obligated to complete extensive security questionnaires or permit audits unless otherwise agreed.

---

13. Continuous Improvement

The Company continually evaluates and improves its security, reliability, and operational practices in response to evolving threats, technology changes, and business needs.

Practices described in this document may change over time and do not constitute fixed commitments.

---

14. No Warranty or Guarantee

This Trust & Security Overview is provided for informational purposes only and does not create any warranties, guarantees, service commitments, or contractual obligations.

End of Trust & Security Overview