SECURITY

Security, Data Protection & Responsible AI Overview

Last Updated: 02/24/2026

This page summarizes Crystal Project Inc.'s ("Crystal") approach to data protection, system security, and responsible use of AI-driven insights.

Crystal provides personality-based communication insights through a purpose-built probabilistic modeling system. Security, privacy, and human oversight are foundational to the platform's design.

1. Data Protection Roles

Crystal acts as a **data processor**. Our customers act as **data controllers**.

Customers determine:

- How and why the platform is used
- What data is entered
- Who has access
- How outputs are applied within their organization

Crystal processes personal data only in accordance with customer instructions and contractual agreements.

Using Crystal does not create a new category of controller responsibility beyond standard SaaS usage.

2. AI System Overview

System Purpose

Crystal provides communication and personality-based insights to support professional interactions.

The platform is purpose-built and is not a general-purpose AI system.

Modeling Approach

Crystal is built on a proprietary Bayesian statistical modeling framework.

The system uses probabilistic inference to estimate likely communication and personality preferences based on observed signals and publicly available professional information.

Outputs are likelihood-based insights and are advisory in nature.

Human Oversight

All system use is initiated by human users.

Crystal does not perform automated decision-making, execute actions, or make determinations without human involvement.

Users are responsible for how insights are applied in their business context.

3. Responsible AI Principles

Crystal's system is designed around the following principles:

- Transparency about system functionality
- Human oversight and user control
- Purpose limitation
- Avoidance of automated decision-making impacting individuals' legal rights
- Aggregate-level performance monitoring

Customer data is not used to train or fine-tune external large language models.

4. Data Sourcing and Processing

Crystal may process:

- Name
- Work email address
- Job title and professional background
- Publicly available professional information

- User-provided inputs

Crystal does not intentionally collect or process special category data such as health data, biometric data, political opinions, religious beliefs, or government identification numbers.

Customers are responsible for ensuring their downstream use of insights complies with applicable laws.

5. Transparency and Customer Responsibilities

Customers are responsible for meeting their own privacy and transparency obligations under applicable laws.

When assessments are used, respondents voluntarily provide information.

For prediction use cases, insights are generated using limited identifiers and publicly available professional information.

Customers determine how transparency requirements apply in their jurisdiction.

6. Security and Infrastructure

Security Program

Crystal maintains a SOC 2 Type II certification covering security controls.

The security program includes:

- Role-based access control, least privilege, and MFA for all workforce identities
- Encryption in transit and at rest
- High-availability cloud architecture with multi-AZ deployment
- Centralized security logging, monitoring, and alerting
- Incident response procedures
- Independent third-party penetration testing performed annually
- Vendor risk management

Hosting Environment

Crystal is hosted on Amazon Web Services (AWS) in the United States.

Production systems are deployed in a multi-availability-zone architecture within the primary AWS region. Crystal relies on AWS physical and infrastructure controls while implementing application-level, identity, and organizational security controls on top of the cloud infrastructure.

Access Controls

Access to customer data is restricted using role-based access controls.

Authorized personnel may access data only for operational, support, or security purposes.

7. Data Rights and Retention

Data Subject Requests

Crystal supports search and export of relevant personal data in structured formats (e.g., CSV, JSON) to assist customers in responding to data subject access requests.

Retention

Data retention is governed by contractual terms and internal data management policies.

Customer data may be deleted upon request, subject to legal or regulatory requirements.

8. Governance and Oversight

Crystal maintains formal governance processes including:

- Risk management and periodic risk reviews
- Secure development and change management controls
- Vulnerability scanning and independent annual penetration testing
- Incident response planning and tabletop exercises
- Disaster recovery planning and resilience testing
- Third-party risk management

No significant security incidents occurred during the most recent SOC 2 Type II audited period.

Additional Documentation

For further documentation, including:

- SOC 2 Type II report
- Data Processing Agreement
- Privacy Policy
- Terms of Service

Please visit our Trust Center or contact:

security@crystalknows.com