General Data Protection Regulation (GDPR)

Revision	Author	Comments	Date
1.0	Ethan Lo	Development of policy	March 2021
1.1	Erica Jansma	Updated standard and template	Apr 5, 2022

185 Berry Street, Suite 6850, San Francisco, CA 94107

415 / 813 - 5464 it-sec@premise.com @premisedata www.premise.com

1. Overview

Premise Data Corporation (Premise) is a crowdsourced data collection, management, and analytics capability. Premise collects and aggregates information about the world using a combination of human data contributors and our cloud-based intelligent computing infrastructure. This document outlines the policies Premise has in place to ensure General Data Protection Regulation (GDPR) compliance.

2. Personal Data Protection Roles and Responsibilities

This section describes the roles and responsibilities pertaining to personal data protection.

2.1. Data Protection Officer

Premise's Data Protection Officer is Mr. Ethan Lo (VP, Platform Engineering). He can be contacted directly (ethan.lo@premise.com) or through the Premise Customer Success Team.

2.2. Personal Data Controller

All decisions regarding the purpose and performance of personal data processing activities and how to safeguard the data collected therefrom are made exclusively by Premise and are independent of any customer. Data control decisions are made by a combination of Premise information security, product management, and legal teams.

2.3. Personal Data Processor

All personal data processing activities are carried out by various Premise engineering teams according to decisions made by Premise information security, product management, and legal teams independent of any customer. Customers cannot instruct Premise to process personal data.

These following principles explain the relationship between Premise, its contributors, and its customers.

- **Premise is an independent controller of the personal data that it collects.** Premise recruits and maintains a network of data contributors globally. This activity is independent from any customer-sponsored tasks.
- **Premise collects personal data for its own quality control and validation purposes. Premise does not share this data with customers.** Personal data is collected and processed when a data contributor signs up to use our mobile app and when performing Premise-sponsored tasks. However, Premise never shares data contributors' personal data with customers or third-party vendors.
- **Personal data is not used to select contributors to answer questions and tasks.** Premise may use location and non-identifiable demographic information to select a subset of data contributors suitable to perform customer-sponsored tasks.

- **Premise will not use Personal Data attributes to select contributors to conduct tasks on behalf of customers.** For the avoidance of doubt, customers cannot instruct Premise to collect data on the basis of personal data attributes.
- **Premise is responsible for safeguarding its data contributors' personal data that it collects.** Premise reserves the right to reject any customer-sponsored tasks that may result in Premise collecting data that can be used by the customer to identify our data contributors.

3. Data Protection and Governance Principles

Premise puts security and data protection at the heart of its corporate culture. Premise adopted and adhered to GDPR principles in advance of their implementation in April 2016 and holds the Cyber Essentials Certification (IASME-CE-009938) .[1]

All Customer Success teams receive regular and extensive training in their responsibilities for handling data and its correct transmission. This is in addition to any system-specific training and onboarding processes for those using government IT systems. Many of our data protection and governance principles are tied to Google Cloud capabilities.[2]

Data protection and governance at Premise are governed by the following principles:

Principle 1: Contributor Anonymity

Premise takes the following steps to ensure anonymity of our data contributors:

- Premise assigns each data contributor a unique anonymised identifier that is used in place of a name.
- Premise never shares contributors' personal data with customers.
- Premise holds data in logically separate areas, separating personal data from sensitive data at all times.
- Device data collected is solely used for fraud detection and cannot be used to identify the data contributors.
- Procedures are in place for data contributors to request destruction of their personal data.

Principle 2: End-to-End Data Encryption Protection

Premise takes the following steps to ensure data is encrypted end-to-end:

- All data collected through the Premise mobile application is secured in transit between the device and Google Cloud using Transport Layer Security (TLS) 1.2+ encryption.
- Data in transit within Google Cloud services and Premise-built microservices is secured using application layer transport security (ALTS) encryption. All data including backup is encrypted at rest using AES-256 and protected from unauthorized access using processes certified under ISO/IEC 2700 and ISO/IEC 27017 international standards.

1 Cyber Essentials Certificate attached

2 To learn more about Google Cloud and GDPR, visit https://www.cloud.google.com/security/gdpr.

Principle 3: Data Location and Legal Jurisdiction

All data collected through and analyzed by the Premise Platform is stored, processed, and managed within the United States of America. The United States of America is also the legal jurisdiction in which Premise Data Corporation operates.

Principle 4: Data Center Security

Google Cloud, Premise's cloud service provider, has had their physical security model measures attested to by the appropriate government authorities in the United States of America. Google Cloud has dedicated teams for information security, physical data center security, and server and software stack security.[3]

Principle 5: Equipment Disposal

Google Cloud, Premise's cloud service provider, is compliant with equipment disposal certifications under ISO/IEC 27001 and ISO/IEC 27017 international standards.

Principle 6: Separation Between Users

All Premise Platform user data is separated at the compute, storage, and networking layers as well as where the services are exposed to customers and at the management interface.

Principle 7: Configuration and Change Management

Google Cloud provides numerous configuration and change management capabilities that are certified under the ISO/EC 27001 and ISO/IEC 24017 international standards. These include the ability to track the status, location, and configuration of service components and assessment of potential security impacts on the service. Premise also maintains a fully auditable change management process.

Principle 8: Security Vulnerability Monitoring and Incident Response

Premise takes the following steps to manage security vulnerabilities and incidents:

- Premise maintains a security monitoring program that uses a mix of Google Cloud security services, security information and event management (SIEM) technology, and built-in-house products that detect and monitor for security vulnerabilities, including but not limited to cross-site-scripting (XSS), flash injection, mixed content (HTTP and HTTPS), outdated/insecure libraries, publicly accessible resources, encryption not being enforced, and abnormal network traffic patterns. All security vulnerabilities are monitored and analyzed by a 24x7 Security Operation Center (SOC).
- Google Cloud has a security incident management program structured around NIST SP 800-61 that has been reviewed as part of their certification under ISO/EC 27001 and ISO/IEC 24017 international standards.
- In the case of a confirmed personal data breach incident, a supervisory authority is notified within 72 hours.

[3] To learn more about Google Cloud's security overview, visit https://cloud.google.com/security/infrastructure/design

Principle 10: Personnel Security

Google Cloud performs security screening for all staff and limits the number of people with access to Premise's hosted encrypted data to the minimum necessary for the purpose of disaster recovery. Google staff do not have the ability to decrypt and see content of Premise's data. Premise maintains roles-based access to both contributor and client-owned data and assigns such access based on an as needed basis using the least privileged model.

Principle 11: Secure Development

All software development at Premise is carried out using industry best practice for secure design, coding, testing, and deployment. Automated tools are continuously performing static and dynamic code analysis. Google Cloud also performed in-house and third-party reviews to ensure their cloud services meet the secure development objectives of their customers.

Principle 12: Supply Chain Security

Google Cloud uses custom, purpose-built servers and network equipment that support supply-chain security and eliminate unnecessary components. The servers run a custom operating system called Container-Optimized OS that is hardened and designed for providing cloud services. These processes and servers are certified under ISO/EC 27001 and ISO/IEC 24017 international standards.

Principle 13: Authentication of Users to Management Interfaces and Support Channels

Google Cloud uses unique identifiers backed by at least annual audits of user authentication certified under ISO 26001:2013, ISO 27-18:2014, and ISO 27017:2015. These are used to control access to mechanisms that would affect the use of services to only authorized individuals.

Principle 14: Separation and Access Control within Management Interfaces

Google Cloud uses unique security backed by at least annual audits of user authentication certified under ISO 26001:2013, ISO 27-18:2014, and ISO 27017:2015. These are used to control access to mechanisms that would affect the use of services to only authorized individuals.

Principle 15: Identity and Authentication

Google Cloud provides Premise with two-step verification that is designed for multi-tenant environments. This provides strong access control and an abstraction level using cryptographic authentication and authorizations at the application layer.