

**Kirin Group
Privacy Data Protection Policy**

Established on December 22, 2020

Kirin Group Privacy Data Protection Policy

In 2018, the Kirin Group formulated the "Kirin Group Human Rights Policy", and has put it into practice since then. The Policy is in line with the "UN Guiding Principles on Business and Human Rights" and is positioned as a high-level policy for all documents and norms related to the Group's initiatives to respect human rights in its business activities.

The Group considers "Personal Information Protection" to be one of the important initiative themes for promoting the practice of respect for human rights, and has newly established the "Kirin Group Privacy Data Protection Policy".

The Group will follow and implement the Policy with the purpose of further promoting business management that protects human rights.

- Policy Scope

- Officers and employees of the Kirin Group

- Position of the Policy

- The Privacy Data Protection Policy functions as the dominant policy for all documents and standards that relate to initiatives for encouraging respect for human rights within the Kirin Group's business activities.

- Outline of Commitments Declared within the Policy

1. Respect and implementation of the eight basic principles of the privacy guidelines adopted by the Organization for Economic Cooperation and Development (OECD)
2. Implementation of continuous improvement initiatives in response to changes in social norms and employee education
3. Periodic announcement of improvements and progress

Kirin Group Privacy Data Protection Policy

1. Implementation of the eight basic principles of the OECD guidelines
Regarding the handling of personal information, we strive to conduct our business activities based on the criteria of whether these principles are conformed to, including the perspective of appropriateness in light of social norms, as well as by complying with the laws of each country.

Principle 1 “Collection Limitation Principle”

When personal data is collected, it should be collected lawfully and through fair means after notifying or obtaining consent from the owner of the personal data.

Principle 2 “Data Quality Principle”

The content of personal data should be in accordance with the purpose of use, accurate, complete, and kept up-to-date.

Principle 3 "Purpose Specification Principle"

The purpose of collecting personal data should be made clear, and any subsequent use should be limited to the fulfilment of such purpose.

Principle 4 “Use Limitation Principle”

The collected data should not be used for any other purpose, excluding cases where the consent of the owner of the personal data is obtained or where it is in accordance with the provisions of law.

Principle 5 "Security Safeguards Principle"

Reasonable security safeguard measures should be taken to protect personal data from loss, destruction, use, modification and leakage, etc.

Principle 6 "Openness Principle"

The personal data collection policy, etc. should be disclosed, and the existence of data, its purpose of use, and the data controller, etc. should be made clear.

Principle 7 "Individual Participation Principle"

It should be ensured that the owner of personal data can confirm the whereabouts and content of the data concerning himself/herself, and he/she should be guaranteed to be able to make an objection.

Principle 8 “Accountability Principle”

A personal data controller should be responsible for implementing the principles stated above.

Kirin Group Privacy Data Protection Policy

2. Implementation of continuous improvement initiatives in response to changes in social norms and employee education

(1) Improvement Based on Social Norm

A mechanism for personal data protection shall be reviewed based on public awareness and trends while taking into consideration moral aspects, and matters to be improved shall be made clear.

(2) Employee Education

Employee education for personal data protection shall be conducted.

3. Periodic announcement of improvements and progress

Information on the progress of the Kirin Group's initiatives shall be published on the Kirin Holdings website.

4. Revision and/or abolition of document

The revision and abolition of this document shall be subject to the approval of the manager of the division responsible for information security management, following discussion within such division. Officers and the workers of the Group Companies shall be informed of any revision and/or abolition.