AA Sakatti Mining Oy, Privacy policy for electronic access control.

Privacy policy in accordance with Articles 13 and 14 of General Data Protection Regulation (EU) 2016/679.

1. Controller

Name of controller	AA Sakatti Mining Oy
Office address	Tuohiaavantie 2, FI-99600 Sodankylä
Business ID/VAT no.	FI24367683
Contact person responsible for the register	Kirsti Kulpakko
Email	kirsti.kulpakko@angloamerican.com

Name of register

Electronic access control system

2. Purpose and legal basis for handling personal data

The purpose of the register and grounds for processing are as follows

1. Compliance with legal obligation and legitimate interest of the controller: Assurance of the safety of persons employed by the company and visitors and protection of property.
2. Electronic access control is performed for ensuring the personal safety of people at the workplace, for monitoring the appropriate functioning of research processes and personal safety, prevention and clarification of situations that compromise safety, property, or research process.

3. Processing of real-time location data is conducted for ensuring the personal safety of employees and contractors working in the terrain, for monitoring the appropriate functioning of research processes and personal safety, prevention and clarification of situations that compromise safety, property, or research process.
4. AA Sakatti Mining Oy (hereinafter referred to as “AASM”) may process personal data and all saved electronic access control material for the purpose of processing compensation claims and legal proceedings.
5. A register is kept of the keys issued and who the keys are issued to. The key control register is based on the person’s employment relationship, customer relationship or contractual relationship.

3. Information held in the register

- Name.
- Employee number.
- Access right group.
- Electronic key stamping data.
- Name and time of visit (manual visitor log).
- Location of GPS transmitter stipulated to be carried by employees working in the terrain.

The electronic access control system creates a personal access code register based on use. Accepted and unaccepted access events, including times and dates, are entered into the access control register.

4. Sources of information for the register

The sources of information for the register are as follows:

- Reading devices for the electronic access control system.
- Location data for GPS transmitters
- On the basis of data received from AASM’s human resource management, the person responsible for the register, or this person’s substitute, shall enter the code holder’s data.
- Manual visitor log filled in by visitors

5. Protection of the register and processing security

The servers intended for storing saved data are located in secure premises fitted with physical security means. Firewalls for protecting the network protect the logical network area.

The register in digital format is protected using passwords. Data is stored in the register for a maximum of three (3) years, unless there is reason to retain the data for a longer period due to special reasons related to video surveillance purposes. Data is removed from the system at regular intervals.

The controller names the persons who are given access rights to the video surveillance videos. Only the person responsible for the system, who has been specifically appointed by the controller for this purpose can grant, alter or cancel these access rights.
Information about video surveillance is notified using signs such as “Recorded video surveillance in progress”, that also include the contact details of the controller.

6. Data disclosure

Data is not disclosed or transferred outside the European Union or European Economic Area.

Data may only be disclosed to the police, or other competent authority, in cases that are separately stipulated in legislation, such as in the cases of resolving criminal acts.

7. The right to inspect and amend information

According to the General Data Protection Regulation, the data subjects held in the register are entitled to have access to what data is collected concerning him or her, and the right to demand rectification or removal of such data (we implement such requests, unless we have legal grounds for not handing over or removing the data). All requests to inspect or rectify data should be sent via email to kirsti.kulpakko@angloamerican.com. The handing over of material is done at an agreed time on the company’s premises and shall be done in person using verification of identity.

8. Miscellaneous rights related to the processing of personal data held in the register

You are entitled to:

- Demand the restriction of the processing of your personal data
- Oppose to the processing of your personal data
- Request for the transfer of personal data you yourself submit from one controller to another
- Cancel any consent you have given, if the processing of personal data is based on consent
- Not to be subject to a decision based on automated processing or profiling

9. Appealing to the supervisory authority

If a data subject feels that the processing of personal data is contrary to applied legislation, or his/her legal rights have been infringed, he/she can issue a complaint to the Data Protection Supervisor.