PRIVACY STATEMENT

Access control and working hours monitoring system

(EU General Data Protection Regulation, Article 30; Personal Data Act (523/1999), sections 10 and 24)

1. Controller

Name	Sámi Parliament
Address	Menesjärventie 2, 99870
Business ID	1052535-3
Contact person	Executive Director Pia Ruotsala-Kangasniemi
Email	pia.ruotsala[at]samediggi.fi
Tel.	+358 40726 2688
Data Protection Officer	Legal Secretary Kalle Varis
Email	kalle.varis[at]samediggi.fi
Tel.	+358 50 384 7040

2. Name of data file

Access control and working hours monitoring system

3. Purpose and legal basis of processing

The purpose of access control is to guarantee the legal protection and safety of Sámi Parliament employees and visitors, protect the privacy of the employer and employees, as well as preventing and investigating crimes. The data stored in the file is used to keep track of the access events of people moving around on the premises and connect them to the correct individuals.

The working hours monitoring system is the working time register required by chapter 7, section 32 of the Working Time Act.

4. Data content of the file

- Name
- Personal identity code
- Access rights group
- Working hours group
- Clock-in and clock-out information

The access control system constitutes a data file based on access card use. Approved and rejected access events are recorded in the access control register with their dates and times.

5. Regular sources of data

The data sources for the file are the reader terminals of the access control system. The person responsible enters the details of the ID holder based on information obtained from the Sámi Parliament's HR administration.

6. Regular disclosures of data and transfers of data outside the EU or EEA

There are no regular disclosures of data or transfers of data outside the EU or EEA.

Data from the access control register is not disclosed regularly to anyone. Data will be disclosed to the police or other competent authorities in cases specifically provided for by law, e.g. for criminal investigations.

7. Technological and organisational safeguards

Use of the access control system is secured with a username and password. Only the user with administrator rights / specifically designated users are able to manage and update the personal data in the system and their related clock-in and clock-out data. The data is stored for the duration of a person's employment. When an employee's employment ends, their access key is cleared of personal data, after which the clock-in and clock-out data remaining in the database can no longer be connected to specific individuals.

8. Right of access and right to rectification of data

Data subjects have the right to inspect their personal data stored in the personal data file and the right to demand the rectification or erasure of their data. Requests to this effect should be delivered in person or in writing to the contact person indicated in section 1.

9. Other rights related to the processing of personal data

Under the GDPR, data subjects have the right to object to processing or request the restriction of processing their data, as well as the right to file a complaint about the processing of their personal data with the supervisory authority.