Security and data protection rules within the Access Card System (SKD)

In this document, we will explain the rules of the Access Card System (**SKD**), including the security of using access cards to designated areas related to the implementation of the Baltic Power investment and the rules for the protection of personal data processed as part of this access control.

I. About the Access Card System

The SKD is a system that monitors entries and exits to areas of particular operational importance managed by us and covered by the SKD, informs about the presence of persons in given zones, allows for the organisation of visits and smooth handling of guests, and monitors logistics processes.

We assign personalised cards to our associates, employees and representatives of our contractors and business partners in accordance with internally established access levels. We also provide cards to visitors.

II. Safety rules

Below are the rules for the safe use of access cards:

1. The access card is personal and assigned exclusively to you. Do not lend or transfer it to third parties, even temporarily.
2. Use access to areas only to the extent necessary to perform your duties or to achieve the purpose of your visit.
3. Keep your card safe. Do not store your card in public places or leave it unattended. In the event of loss, theft or damage to your card, immediately report this to the security staff and the administrator of the Service Base building in Łeba.
4. Do not allow the access control system to be circumvented (e.g. entering with another person, using someone else's card).
5. As an access card holder, you are required to comply with all safety instructions applicable in protected areas.
6. If you notice anything unusual (e.g. an open door in a restricted area), please inform security personnel.
7. In the event of a system failure or card problems, follow the instructions of the security staff .
8. Each use of the card is recorded in the SKD software.

Contact number for security personnel: +48 502 458 681

III. Information on the processing of personal data within the SKD

1. Who is the controller of your personal data?

The controller of your personal data is Baltic Power spółka z ograniczoną odpowiedzialnością with its registered office in Warsaw, ul. Bielańska 12, 00-085 Warsaw, entered in the Register of Entrepreneurs under KRS number 0000400905, NIP 5272668625, REGON 145868460 (**us**).

2. How can you contact us?

In matters relating to the processing of your personal data, you can contact us:

a) by sending traditional correspondence to the following address: ul. Bielańska 12 Warsaw 00-085, or

b) via e-mail: blp.leba.office@balticpower.pl

3. What personal data do we process and from what sources? Is it necessary to provide us with personal data?

We will process your personal data necessary for the proper configuration and functioning of the Access Card System. This may include, in particular, your first name, surname and car registration number.

If you are our employee or a member of our contractor's staff, we will also process your image (photo), information about your position and the details of our contractor for whom you work.

In addition, the system monitors your entries and exits from areas covered by the SKD, informs about the presence of people in specific zones, allows for the organisation of visits and smooth handling of guests, and monitors logistics processes.

We obtain personal data directly from you, unless we already have it in connection with our business relationship.

Providing personal data is necessary for us to grant you access to the areas of strategic importance that we manage. Failure to provide us with personal data will result in you being unable to enter/drive into the SKD area.

4. For what purposes and on what legal basis do we process your personal data?

Your personal data will be processed for the purposes of our legitimate interests, consisting in configuring and providing you with an access card, and then controlling access to and securing the areas of particular operational importance that we manage, ensuring the protection and safety of persons and property there, as well as the need to ensure the confidentiality of information whose disclosure could expose us or other entities to harm, i.e. on the legal basis of Article 6(1)(f) of the GDPR.

In addition, we may process personal data obtained through the SKD for the purpose of establishing, pursuing or defending against claims, as part of our legitimate interest in being able to defend or exercise our rights, i.e. on the legal basis of Article 6(1)(f) of the GDPR.

5. How long do we store your personal data?

If you are our employee or a member of our subcontractor's (contractor's) staff and you have received a permanent card, we will store your personal data from this card for the duration of our cooperation or our cooperation with your employer and our subcontractor.

If you are a visitor and have received a visitor card, we will store your personal data from this card for a period of one full calendar month from the date of your last visit to us under the visitor card issued to you.

In turn, we store your personal data covered by records, reports and other information generated within the SKD system for a period of two years.

However, in the event that the records from the system constitute evidence in proceedings conducted on the basis of the law, or we become aware that they may constitute evidence in proceedings, the period specified in the previous sentence will be extended until the proceedings are legally concluded.

6. Who can we share your personal data with?

We may transfer your personal data to entities providing services to us, including Access Card System (SKD) providers, IT service providers, personal and property security service providers, occupational health and safety service providers, legal advisors and entities authorised under generally applicable law, in particular institutions authorised to control our activities or institutions authorised to obtain personal data under the law.

7. Do we transfer your personal data outside the EEA?

We process your personal data within the EEA. The EEA is the European Economic Area, i.e. the European Union, as well as Iceland, Norway and Liechtenstein.

However, some of our service providers (due to the global nature of their services) may process your personal data outside the EEA. In such cases, we secure the transfer of data outside the EEA in accordance with data protection regulations. We typically use the European Commission's standard contractual clauses or work with entities participating in the EU-US Data Privacy Framework (for transfers to the US). We also assess such data transfers for security in accordance with legal requirements.

If you would like to learn more about the safeguards we use for data transfers outside the EEA, including obtaining a copy of such safeguards, please contact us (our contact details are provided in section 2 of this notice).

8. What are your rights?

You have the following rights in relation to the processing of your personal data:

a) access to your data, including obtaining a copy of your data,

b) rectification of data,

c) deletion of data - we will delete your personal data if there are no reasons for which we are obliged or have a legitimate interest to store it, e.g. we may

retain certain information about you to the extent necessary for the purposes of establishing,
pursuing or defending claims,

d) restrict data processing, and

e) the right to object to data processing. We will take your objection into account if it is justified (after weighing our and your interests and rights).

You have the above rights in the cases and to the extent provided for by applicable legal provisions.

You also have the right to lodge a complaint with the supervisory authority – the President of the Personal Data Protection Office. For more information, please visit: https://www.uodo.gov.pl/pl/526/2464.

9. Do we use profiling or automated decision-making?

We do not make automated decisions based on your personal data, nor do we engage in profiling.