Rules for the use of video surveillance, together with information on the processing of personal data

In this document, we will explain the rules for the use of video surveillance on the premises and in the offices managed by Baltic Power, as well as the rules for the protection of personal data processed as part of surveillance.

I. What does our surveillance involve?

Due to the specific security requirements and strategic nature of our infrastructure, the use of surveillance is necessary to ensure an adequate level of protection.

Video surveillance is a tool used to increase the safety of people and property and to ensure the proper functioning of processes at Baltic Power. Its use is preventive in nature and its purpose is to protect against threats such as unauthorised access to facilities, sabotage, theft or events that may cause losses.

We use video surveillance in a proportionate manner, respecting the privacy and dignity of individuals, in accordance with applicable laws and ethical principles.

We have conducted a legitimate interest test to assess whether the use of surveillance is consistent with the principle of proportionality and does not violate the rights and freedoms of the persons covered by the recordings. The conclusions of the analysis confirmed that surveillance is a proportionate measure and complies with applicable regulations, and that the safeguards in place minimise the impact on individuals' rights.

II. What are the rules for using video surveillance?

1. Video surveillance in designated areas supervised by Baltic Power is managed by Baltic Power Limited Liability Company (**us**).
2. Surveillance is conducted 24 hours a day.
3. Cameras are installed only in places where it is justified for security reasons.
4. Video surveillance covers the outdoor areas managed by us, including the offshore wind farm area and buildings, e.g. office buildings, warehouses, etc. Surveillance in office buildings covers only passageways.
5. Areas covered by monitoring are appropriately marked with signs informing about image recording.
6. Access to recordings is strictly limited to authorised persons and may be granted to external entities only in justified cases (more information below in the Rules for the processing of personal data from video surveillance).
7. Current access to monitoring recordings is granted to employees of the company providing personal and property security services on the basis of a personal data processing agreement concluded with Baltic Power.

8. Persons with access to CCTV recordings are obliged to comply with regarding personal data protection.

III. Rules for the processing of personal data from video surveillance

1. Who is the controller of personal data in the context of monitoring?

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. Whose data do we process as part of video surveillance and what kind of data is it?

As part of video surveillance, we process **images** of persons covered by surveillance (surveillance does not include sound). These may include, in particular, our employees, the staff of our subcontractors, suppliers and other contractors, as well as persons visiting our premises and facilities.

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

We process personal data from video surveillance for the purpose of pursuing our legitimate interests, which consist in controlling access to the premises and facilities managed by Baltic Power and ensuring the protection and safety of persons and property there, as well as the need to keep confidential information that could cause harm if disclosed, i.e. on the legal basis of Article 6(1)(f) of the GDPR.

To the extent that monitoring covers areas of strategic importance for the wind farm infrastructure, personal data may also be processed on the basis of Article 6(1)(e) of the GDPR, i.e. for the performance of a task carried out in the public interest, consisting in ensuring the security of infrastructure of significant social importance, including its protection against threats during construction.

In addition, we may process personal data obtained through monitoring 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 personal data from video surveillance?

We will store personal data from video surveillance for a period of 30 days from the date of recording. In cases where the image recordings constitute evidence in

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

6. To whom may we disclose personal data from video surveillance?

Video surveillance recordings may be made available to entities authorised by law, in particular institutions authorised to obtain personal data under the law, as well as our service providers (e.g. security services, IT services). In justified cases, the recordings may be made available to our subcontractors or partners if this is necessary for the performance of services for the controller or for the protection of their rights, while maintaining security rules and in accordance with applicable law.

7. Do we transfer personal data outside the EEA?

We process your personal data on within the EEA. The EEA is the European Economic
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, e.g. cloud services) may process your personal data outside the EEA. In such cases, we secure data transfers 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 against claims,

d) restriction of data processing, and

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

The above rights are available to you in cases and to the extent provided for by
applicable law.

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.