

Zasady stosowania monitoringu wizyjnego wraz z informacją o przetwarzaniu danych osobowych

W tym dokumencie przybliżymy Ci zasady stosowania monitoringu wizyjnego na terenach i w biurach zarządzanych przez Baltic Power oraz zasady ochrony danych osobowych przetwarzanych w ramach monitoringu.

I. Na czym polega nasz monitoring?

Ze względu na szczególne wymagania związane z bezpieczeństwem oraz strategiczny charakter naszej infrastruktury, stosowanie monitoringu jest niezbędne dla zapewnienia właściwego poziomu ochrony.

Monitoring wizyjny jest narzędziem służącym zwiększeniu bezpieczeństwa osób i mienia oraz zapewnieniu prawidłowego funkcjonowania procesów w Baltic Power. Jego stosowanie ma charakter prewencyjny, a celem jest ochrona przed zagrożeniami, takimi jak nieuprawniony dostęp do obiektów, działania sabotażowe, kradzieże czy zdarzenia mogące narażać na straty.

Stosujemy monitoring wizyjny w sposób proporcjonalny, z poszanowaniem prywatności i godności osób, zgodnie z obowiązującymi przepisami prawa i zasadami etyki.

Przeprowadziliśmy test uzasadnionego interesu, aby ocenić, czy stosowanie monitoringu jest zgodne z zasadą proporcjonalności i nie narusza praw oraz wolności osób objętych nagraniami. Wnioski z analizy potwierdziły, że monitoring jest środkiem proporcjonalnym i zgodnym z obowiązującymi przepisami, a stosowane zabezpieczenia minimalizują wpływ na prawa osób.

II. Jakie są zasady stosowania monitoringu wizyjnego?

1. Monitoringiem wizyjnym w wyznaczonych obszarach nadzorowanych przez Baltic Power zarządza Baltic Power spółka z ograniczoną odpowiedzialnością (**my**).
2. Monitoring jest całodobowy.
3. Kamery są instalowane wyłącznie w miejscach, gdzie jest to uzasadnione względami bezpieczeństwa.
4. Monitoringiem wizyjnym objęte są zarządzane przez nas tereny zewnętrzne, m.in. obszar MFW oraz budynki, np. biurowe, hale magazynowe itd. Monitoring w budynkach biurowych obejmuje wyłącznie ciągi komunikacyjne.
5. Obszary objęte monitoringiem są odpowiednio oznaczone znakami informacyjnymi o rejestracji obrazu.
6. Dostęp do nagrań jest ściśle ograniczony do osób upoważnionych i może być udzielany podmiotom zewnętrznym tylko w uzasadnionych przypadkach (więcej informacji poniżej w Zasadach przetwarzania danych osobowych z monitoringu wizyjnego).
7. Bieżący dostęp do nagrań monitoringu mają pracownicy firmy świadczącej usługi ochrony osób i mienia na podstawie umowy powierzenia danych osobowych zawartej z Baltic Power.

8. Osoby mające wgląd w nagrania monitoringu zobowiązane są do przestrzegania przepisów prawa w zakresie ochrony danych osobowych.

III. Zasady przetwarzania danych osobowych z monitoringu wizyjnego

1. Kto jest administratorem danych osobowych w ramach monitoringu?

Administratorem Twoich danych osobowych jest **Baltic Power spółka z ograniczoną odpowiedzialnością** z siedzibą w Warszawie, ul. Bielańska 12, 00-085 Warszawa, wpisana do rejestru przedsiębiorców pod numerem KRS 0000400905, NIP 5272668625, REGON 145868460 (my).

2. Jak możesz się z nami skontaktować?

W sprawach dotyczących przetwarzania Twoich danych osobowych możesz się z nami skontaktować:

- a) kierując korespondencję tradycyjną na adres: ul. Bielańska 12 Warszawa 00-085, lub
- b) za pośrednictwem adresu e-mail: blp.leba.office@balticpower.pl

3. Czyje i jakie dane przetwarzamy w ramach monitoringu wizyjnego?

W ramach monitoringu wizyjnego przetwarzamy **wizerunek** osób objętych zasięgiem monitoringu (monitoring nie obejmuje dźwięku). Mogą to być w szczególności nasi współpracownicy, personel naszych podwykonawców, dostawców i innych kontrahentów oraz osoby odwiedzające nasze tereny i obiekty.

4. W jakich celach i na jakich podstawach prawnych przetwarzamy dane osobowe z monitoringu?

Dane osobowe w ramach monitoringu wizyjnego przetwarzamy w celu realizacji naszych prawnie uzasadnionych interesów polegających na kontroli dostępu na tereny i obiekty zarządzane przez Baltic Power oraz zapewnienia ochrony i bezpieczeństwa osób tam przebywających oraz mienia, a także polegających na potrzebie zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić na szkodę, tj. na podstawie prawnej z art. 6 ust. 1 lit. f) RODO.

W zakresie, w jakim monitoring obejmuje obszary strategiczne dla infrastruktury farmy wiatrowej, dane osobowe mogą być przetwarzane również na podstawie art. 6 ust. 1 lit. e RODO, tj. w celu wykonania zadania realizowanego w interesie publicznym, polegającego na zapewnieniu bezpieczeństwa infrastruktury o istotnym znaczeniu społecznym, w tym jej ochrony przed zagrożeniami w trakcie budowy.

Ponadto dane osobowe pozyskiwane w ramach monitoringu możemy przetwarzać w celu ewentualnego ustalenia, dochodzenia roszczeń lub obrony przed roszczeniami, w ramach naszego prawnie uzasadnionego interesu polegającego na możliwości obrony lub realizacji naszych praw, tj. na podstawie prawnej z art. 6 ust. 1 lit. f) RODO.

5. Jak długo przechowujemy dane osobowe z monitoringu wizyjnego?

Dane osobowe pochodzące z monitoringu wizyjnego będziemy przechowywać przez okres 30 dni od dnia nagrania. W przypadku, w którym nagrania obrazu będą stanowiły dowód w

postępowaniu prowadzonym na podstawie prawa lub poweźmiemy wiadomość, że mogą one stanowić dowód w postępowaniu, termin wskazany w zdaniu poprzednim ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

6. Komu możemy przekazać dane osobowe z monitoringu wizyjnego?

Nagrania z monitoringu wizyjnego mogą być udostępnione podmiotom upoważnionym na podstawie przepisów prawa, w szczególności instytucjom uprawnionym do uzyskania danych osobowych na podstawie przepisów prawa, a także naszym dostawcom usług (np. usługi ochroniarskie, usługi IT). W uzasadnionych przypadkach nagrania mogą zostać udostępnione naszym podwykonawcom lub partnerom, jeżeli jest to niezbędne do realizacji usług na rzecz administratora albo do ochrony ich praw, przy zachowaniu zasad bezpieczeństwa i zgodnie z obowiązującymi przepisami prawa.

7. Czy przekazujemy dane osobowe poza EOG?

Twoje dane osobowe przetwarzamy na terenie EOG. EOG to Europejski Obszar Gospodarczy, czyli Unia Europejska, a także Islandia, Norwegia i Liechtenstein.

Jednak może się zdarzyć, że niektórzy z naszych usługodawców (z uwagi na globalny charakter ich usług, np. usługi chmurowe) mogą przetwarzać Twoje dane osobowe poza EOG. W takiej sytuacji zabezpieczamy transfer danych poza EOG zgodnie z przepisami o ochronie danych osobowych. Zwykle stosujemy standardowe klauzule umowne Komisji Europejskiej lub współpracujemy z podmiotami uczestniczącymi w programie EU-US Data Privacy Framework (w odniesieniu do transferów do USA). Oceniamy też takie transfery danych pod kątem bezpieczeństwa zgodnie z wymaganiami prawnymi.

Jeżeli chcesz dowiedzieć się więcej na temat zabezpieczeń, jakie stosujemy w ramach transferów danych poza EOG, w tym uzyskać kopię takich zabezpieczeń, skontaktuj się z nami (dane kontaktowe wskazaliśmy w punkcie 2 tej informacji).

8. Jakie prawa Ci przysługują?

Przysługują Ci następujące prawa w związku z przetwarzaniem Twoich danych osobowych:

- dostępu do danych, w tym uzyskania kopii danych,
- sprostowania danych,
- usunięcia danych - usuniemy Twoje dane osobowe, jeżeli nie istnieją powody, dla których mamy obowiązek lub prawnie uzasadniony interes je przechowywać, np. możemy zachować pewne informacje o Tobie w zakresie niezbędnym do celów ustalenia, dochodzenia lub obrony przed roszczeniami,
- ograniczenia przetwarzania danych oraz
- prawo do sprzeciwu wobec przetwarzania danych. Uwzględnimy Twój sprzeciw, jeżeli będzie zasadny (po zważeniu interesów oraz praw).

Powyższe prawa przysługują Ci w przypadkach i w zakresie przewidzianym przez obowiązujące przepisy prawa.

Przysługuje Ci również prawo do wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, więcej informacji pod tym linkiem: <https://www.uodo.gov.pl/pl/526/2464>.



9. Czy stosujemy profilowanie lub automatyczne podejmowanie decyzji?

Nie podejmujemy automatycznych decyzji w oparciu o Twoje dane osobowe ani nie dokonujemy profilowania.