

KLAUZULA INFORMACYJNA

dotycząca przetwarzania danych osobowych w związku z zarządzaniem bezpieczeństwem informacji i incydentami

Dyrektywa NIS2 (2022/2555) — art. 13 Rozporządzenia (UE) 2016/679 (RODO)

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) informujemy:

| | |
|---|---|
| 1. Administrator danych | Zakład Gospodarki Komunalnej i Mieszkaniowej w Słomnikach (ZGKiM), ul. Tadeusza Kościuszki 64, 32-090 Słomniki, e-mail: zgkim@slomniki.pl |
| 2. Inspektor Ochrony Danych (IOD) | Z Inspektorem Ochrony Danych można skontaktować się pisemnie na adres administratora lub drogą e-mail: kontakt@inspektordanych.com.pl lub iod.slomniki@gmail.com |
| 3. Kategorie przetwarzanych danych | W związku z realizacją obowiązków z zakresu cyberbezpieczeństwa ZGKiM może przetwarzać: <ul style="list-style-type: none">– dane osób zgłaszających incydent: imię i nazwisko, stanowisko, dane kontaktowe;– dane techniczne osób, których dotyczy incydent: adresy IP, loginy systemowe, logi aktywności (w zakresie niezbędnym do analizy incydentu);– dane osób zaangażowanych w obsługę incydentu: pracownicy ZGKiM, podmioty zewnętrzne (dostawcy IT, CSIRT). |
| 4. Cele i podstawy prawne przetwarzania | Dane osobowe przetwarzane są w następujących celach: <ul style="list-style-type: none">– zgłoszenie incydentu do właściwego CSIRT (CERT Polska) i organu nadzoru w terminach określonych przez ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa implementującą Dyrektywę NIS2 (2022/2555) — art. 6 ust. 1 lit. c RODO;– zarządzanie incydentami bezpieczeństwa, analiza przyczyn i wdrożenie środków naprawczych — art. 6 ust. 1 lit. c RODO;– zapewnienie ciągłości działania infrastruktury krytycznej zaopatrzenia w wodę — art. 6 ust. 1 lit. e RODO (zadanie w interesie publicznym);– udokumentowanie zdarzeń dla celów audytu i dowodowych — art. 6 ust. 1 lit. c RODO.– kontakt w sprawach związanych z realizacją celów przetwarzania, w zakresie dobrowolnie podanego numeru telefonu i adresu e-mail — na podstawie zgody (art. 6 ust. 1 lit. a RODO). |
| 5. Okres przechowywania danych | Dane osobowe przechowywane są przez: <ul style="list-style-type: none">– 5 lat od zakończenia obsługi incydentu — dokumentacja incydentów bezpieczeństwa, zgodnie z wymogami ustawy o KSC;– okres wymagany zgodnie z jednolitym rzeczowym wykazem akt oraz rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej — pozostała dokumentacja z zakresu cyberbezpieczeństwa;– do czasu prawomocnego zakończenia postępowania — jeśli incydent stał się przedmiotem postępowania karnego lub cywilnego.– do czasu cofnięcia zgody lub ustąpienia celu przetwarzania — w zakresie dobrowolnie podanego numeru telefonu i adresu e-mail (art. 6 ust. 1 lit. a RODO). |
| 6. Odbiorcy danych | Dane mogą być przekazane: <ul style="list-style-type: none">– CSIRT GOV / CERT Polska — w ramach obowiązkowego zgłaszania incydentów;– ministrowi właściwemu do spraw informatyzacji i organom nadzorczym;– podmiotom przetwarzającym dane na podstawie umów powierzenia (obsługa IT, dostawcy systemów bezpieczeństwa);– organom ścigania — w razie podejrzenia popełnienia przestępstwa. |
| 7. Przekazywanie danych do państw trzecich | Dane osobowe nie będą przekazywane do państw trzecich (poza Europejski Obszar Gospodarczy) ani organizacjom międzynarodowym. |
| 8. Prawa osoby, której dane dotyczą | Przysługuje Pani/Panu prawo do: <ul style="list-style-type: none">– dostępu do treści swoich danych oraz uzyskania kopii (art. 15 RODO);– sprostowania danych (art. 16 RODO);– usunięcia danych — o ile nie zachodzi nadrzędna podstawa prawna dalszego przetwarzania (art. 17 RODO);– ograniczenia przetwarzania (art. 18 RODO);– przenoszenia danych — wyłącznie w zakresie przetwarzania na podstawie art. 6 ust. 1 lit. b RODO, gdy przetwarzanie odbywa się w sposób zautomatyzowany (art. 20 RODO);– wniesienia sprzeciwu wobec przetwarzania opartego na prawnie uzasadnionym interesie (art. 6 ust. 1 lit. f RODO) — art. 21 RODO. Uwaga: realizacja praw może być ograniczona w zakresie, w jakim dane są niezbędne do wywiązania się z obowiązków prawnych w zakresie cyberbezpieczeństwa lub stanowią materiał dowodowy w prowadzonym postępowaniu (art. 17 ust. 3 lit. b i e RODO). <ul style="list-style-type: none">– cofnięcia zgody na przetwarzanie numeru telefonu i adresu e-mail w dowolnym momencie — bez wpływu na zgodność z prawem przetwarzania dokonanego przed jej cofnięciem (art. 7 ust. 3 RODO). |

| | |
|--|---|
| 9. Prawo wniesienia skargi | Przysługuje Pani/Panu prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (www.uodo.gov.pl) w przypadku uznania, że przetwarzanie danych narusza przepisy RODO. |
| 10. Obowiązek / dobrowolność podania danych | Przetwarzanie danych w tym zakresie wynika z obowiązków prawnych nałożonych na ZGKiM jako podmiot istotny w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa. Podanie danych przez osoby zgłaszające incydent jest niezbędne do jego prawidłowej obsługi i dokumentacji. |
| 11. Zautomatyzowane podejmowanie decyzji | Dane osobowe nie będą przetwarzane w sposób zautomatyzowany (w tym profilowane) w rozumieniu art. 22 RODO. |