NAJWYŻSZA IZBA KONTROLI

Delegatura w Białymstoku

LBI.411.003.12.2023

Pan
Jerzy Iwanowiec
Wójt Gminy Milejczyce
Urząd Gminy Milejczyce
ul. Szkolna 5, 17-332 Milejczyce

WYSTĄPIENIE POKONTROLNE

I/23/002 – Zapewnienie ochrony i prawidłowego przetwarzania danych, w tym danych osobowych gromadzonych w formie elektronicznej przez jednostki samorządu terytorialnego oraz podległe jednostki organizacyjne na stronach internetowych, poczcie elektronicznej oraz w związku z odbywającymi się sesjami organów uchwałodawczych

NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku
ul. Akademicka 4, 15-267 Białystok
T +48 85 874 81 00, F +48 85 874 81 33
lbi@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Urząd Gminy Milejczyce, ul. Szkolna 5, 17-332 Milejczyce[1]
Kierownik jednostki kontrolowanej	Jerzy Iwanowiec, Wójt Gminy Milejczyce[2]
Zakres przedmiotowy kontroli	Zapewnienie ochrony i prawidłowego przetwarzania danych, w tym danych osobowych gromadzonych w formie elektronicznej przez jednostki samorządu terytorialnego oraz podległe jednostki organizacyjne na stronach internetowych, poczcie elektronicznej oraz w związku z odbywającymi się sesjami organów uchwałodawczych.
Okres objęty kontrolą	Lata 2018-2022 z uwzględnieniem dowodów sporządzonych przed i po tym okresie, jeżeli miały one związek z przedmiotem kontroli.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. *o Najwyższej Izbie Kontroli*[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Białymstoku
Kontroler	Mariusz Lenkiewicz, doradca ekonomiczny, upoważnienia do kontroli nr LBI/60/2023 z 9 marca 2023 r. (akta kontroli str. 1-2)

[1] Dalej: Urząd lub UG Milejczyce.
[2] Pełniący funkcję Wójta od 28 listopada 2014 r.
[3] Dz. U. z 2022 r. poz. 623. Ustawa zwana dalej: *ustawą o NIK*.

II. Ocena ogólna kontrolowanej działalności[4]

OCENA OGÓLNA

W latach 2018-2022 Wójt jako kierownik Urzędu i zwierzchnik służbowy kierowników gminnych jednostek organizacyjnych prowadził na ogół skuteczne działania, które gwarantowały odpowiedni poziom bezpieczeństwa danych, w tym danych osobowych gromadzonych przez Urząd w formie elektronicznej lecz nie realizował skutecznej i adekwatnej kontroli zarządczej w tym zakresie na poziomie jednostki samorządu terytorialnego (gminy).

W Urzędzie wykorzystywano w sposób zgodny z przepisami prawa pocztę mailową do przechowywania i przetwarzania danych, w tym danych osobowych. W dwóch[5] (z czterech) gminnych jednostkach organizacyjnych stwierdzono jednak wieloletnie (w latach 2018-2022) gromadzenie poczty elektronicznej zawierającej dane osobowe z wykorzystaniem usługi hostingu na komercyjnych domenach internetowych. Odbywało się to bez zawarcia stosownej umowy powierzenia przetwarzania danych osobowych z podmiotem przetwarzającym wymaganej art. 28 ust. 3 rozporządzenia *Parlamentu Europejskiego i Rady UE 2016/679 i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE*[6]. Transmitowanie i upublicznianie przez Urząd sesji organu uchwałodawczego odbywało się za pośrednictwem serwisu, z właścicielem którego podpisano umowę powierzenia przetwarzania danych osobowych, jednocześnie przy zastosowaniu transkrypcji wymaganej od 23 września 2020 r. przepisami prawa dotyczącymi dostępności cyfrowej[7]. Na odpowiedni stopień bezpieczeństwa przetwarzanych w Urzędzie danych osobowych wpływ miało też gromadzenie i upublicznianie danych osobowych w oświadczeniach majątkowych na stronie internetowej Biuletynu Informacji Publicznej przez okres wskazany w *ustawie z dnia 8 marca 1990 r. o samorządzie gminnym*[8]. Tym niemniej, w trzech przypadkach, Urząd – stosując nieprawidłowy sposób anonimizacji – umożliwił odczytanie danych osobowych m.in. osób skarżących działalność organu lub kierownika jednostki samorządowej w treści uchwały bez zachowania zasady minimalizowania danych osobowych określonej w art. 5 ust. 1 lit. c *ogólnego rozporządzenia o ochronie danych.*

Już w trakcie kontroli NIK – od marca do maja 2023 roku – Urząd podjął szereg działań naprawczych celem zapewnienia pełnej ochrony danych będących przedmiotem niniejszej kontroli. W ich konsekwencji wszystkie stany nieprawidłowe stwierdzone w zakresie przetwarzania danych osobowych na stronach internetowych i poczcie elektronicznej zostały usunięte zarówno w Urzędzie jak i gminnych jednostkach organizacyjnych.

III. Opis ustalonego stanu faktycznego

OBSZAR

Zapewnienie ochrony i prawidłowego przetwarzania danych, w tym danych osobowych gromadzonych w formie elektronicznej przez jednostki samorządu terytorialnego oraz podległe jednostki organizacyjne na stronach internetowych, poczcie elektronicznej oraz w związku z odbywającymi się sesjami organów uchwałodawczych

Opis stanu faktycznego

W latach 2018-2022 UG Milejczyce wykorzystywał jeden główny adres mailowy gmina@milejczyce.pl i zawarł umowę powierzenia przetwarzania danych osobowych z usługodawcą oferującym hosting i domenę. Na tej skrzynce pocztowej gromadzono i przetwarzano dane osobowe, tj. Imię i nazwisko, wiek, płeć, PESEL, nr telefonu, adres e-mail, numer REGON, Numer NIP, stan cywilny. Pracownicy Urzędu korzystali z imiennych skrzynek e-mailowych w domenie *@milejczyce.pl*.

---

[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[5] W Gminnym Ośrodku Pomocy Społecznej w Milejczycach i Szkole Podstawowej w Milejczycach.

[6] Rozporządzenie zwane w dalszej części wystąpienia pokontrolnego *ogólnym rozporządzeniu o ochronie danych* lub *RODO.*

[7] Zgodnie z wymogami *ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych* (Dz. U. z 2019 r., poz. 848). Ustawa zwana w dalszej części wystąpienia pokontrolnego *ustawą o dostępności stron internetowych.*

[8] Dz. U. z 2023 r. poz. 40, ze zm. Ustawa zwana dalej *ustawą o samorządzie gminnym.*

W latach 2018-2022 Wójt nie prowadził skutecznej i adekwatnej kontroli zarządczej w gminnych jednostkach organizacyjnych w zakresie bezpieczeństwa danych, w tym danych osobowych gromadzonych przez te jednostki w formie elektronicznej. Dwie (z czterech) gminne jednostki organizacyjne posiadały w tym okresie główne skrzynki poczty elektronicznej na komercyjnych domenach internetowych bez zawarcia stosownej umowy powierzenia przetwarzania danych osobowych z podmiotem przetwarzającym stosownie do wymogów art. 28 ust. 3 *RODO*[9]. Na wszystkich głównych skrzynkach mailowych jednostek organizacyjnych przetwarzano głównie dane osobowe zwykłe, przede wszystkim imię, nazwisko, adres, itp. Kategorie osób, których dane były przewarzane za pośrednictwem tych skrzynek mailowych zależne były od charakteru zadań realizowanego przez jednostki podległe i byli to m.in. pracownicy administratora danych osobowych, kontrahenci i klienci.

Jak wyjaśnił Wójt przyczyną stwierdzanych nieprawidłowości dotyczących użytkowania w podległych Urzędowi jednostkach podległych skrzynek mailowych na domenach komercyjnych bez zawarcia stosownych umów powierzenia przetwarzania danych osobowych były zbyt długie i skomplikowane adresy mailowe na posiadanej przez Urząd (i jednostki podległe) domenie *ug.milejczyce.wrotapodlasia.pl.*

NIK zwraca uwagę, że w świetle art. 4 pkt 7 RODO oraz art. 8 i 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[10] wszystkie gminne jednostki organizacyjne jako podmioty sektora finansów publicznych są samodzielnymi administratorami danych i ustanowiły odrębnych inspektorów danych, o których mowa w art. 37-39 RODO i w art. 9 uodo. Nie skorzystano z możliwości wyznaczenia jednego inspektora ochrony danych dla tych jednostek, przewidzianej w art. 37 ust. 3 RODO i w art. 10 ust. 5 uodo. Niemniej, dla zabezpieczenia danych osobowych, przetwarzanych w gminie jako jednostce samorządu terytorialnego w związku z wykonywaniem zadań publicznych jej przypisanych wskazane jest wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających bezpieczeństwo przetwarzania tych danych zarówno w Urzędzie jak i we wszystkich gminnych jednostkach organizacyjnych. W przypadku korzystania z hostingu i domeny usługodawcy zewnętrznego środkiem takim jest zawarcie umowy powierzenia przetwarzania danych osobowych, zapewniającej odpowiednie bezpieczeństwo danych m.in. w zakresie: [1] przetwarzania danych wyłącznie na udokumentowane polecenie administratora; [2] zobowiązania podmiotu przetwarzającego do zachowania tajemnicy; [3] usunięcia (lub zwrotu) wszelkich danych osobowych po zakończeniu świadczenia usługi oraz innych zobowiązań określonych w art. 28 ust. 3 *RODO*.

Wójt – będący zgodnie z art. 33 ust. 3 i 5 ustawy o samorządzie gminnym kierownikiem Urzędu i zwierzchnikiem służbowym kierowników gminnych jednostek organizacyjnych – powinien zawrzeć taką umowę, dotyczącą Urzędu oraz zapewnić – w ramach kontroli zarządczej sprawowanej na poziomie jednostki samorządu terytorialnego stosownie do art. 69 ust. 1 pkt 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[11] i do części I.2.3 – I.2.6 Standardów kontroli zarządczej dla sektora finansów publicznych[12] – aby umowy takie zawarte zostały przez wszystkie gminne jednostki organizacyjne.

NIK zwraca też uwagę, że dwie z czterech jednostek organizacyjnych Gminy Milejczyce funkcjonuje w ramach osobowości prawnej tej Gminy, zaś zgodnie z motywem 146 oraz z art. 79 i 82 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO ma prawo uzyskać – dochodzone przed właściwym sądem – odszkodowanie od administratora, niezależnie od dostępnych administracyjnych lub pozasądowych środków ochrony prawnej. W sytuacji, gdy roszczenie to ma charakter cywilnoprawny, osobą zobowiązaną byłaby gmina jako osoba prawna. (akta kontroli str. 3-18)

2. Na stronie internetowej http://bip.ug.milejczyce.wrotapodlasia.pl/ UG Milejczyce prowadziło Biuletyn Informacji Publicznej (BIP) i zawarło z właścicielem tego serwisu stosowną umowę powierzenia przetwarzania danych osobowych. W BIP publikowane były m.in. oświadczenia majątkowe osób, o których mowa w art. 24h ust. 1 ustawy o samorządzie

---

[9] W Szkole Podstawowej w Milejczycach użytkowano głównego konta poczty elektronicznej zsmilejczyce@gmail.com, w Gminnym Ośrodku Pomocy Społecznej – gopsmilejczyce@wp.pl.

[10] Dz. U. z 2019 r. poz. 1781. Dalej: uodo.

[11] Dz. U. z 2022 r. poz. 1634, ze zm.

[12] Ogłoszonych Komunikatem Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. (Dz. Urz. MF Nr 15, poz. 84)

gminnym, które stosownie do art. 24h ust. 6 tej ustawy, przechowuje się przez okres sześciu lat. Nie stwierdzono przypadku przechowywania oświadczenia majątkowego zawierającego dane osobowe przez dłuższy okres, niż wynikający z art. 24h ust. 6 ustawy o samorządzie gminnym. (akta kontroli str. 3-5, 13-15, 155-159)

3. Do realizowania obowiązku publikacji sesji organu uchwałodawczego wynikającego z art. 20 ust. 1b ustawy o samorządzie gminnym Urząd wykorzystywał serwis *Telewizji Powiatowej,* z właścicielem którego zawarto umowę powierzenia przetwarzania danych osobowych. Upubliczniane w portalu sesje Rady Gminy zawierały wymaganą transkrypcję, co było zgodne z wymogiem dostępności cyfrowej (od 23 września 2020 r.) określonym w *ustawie o dostępności stron internetowych.* (akta kontroli str. 3-5, 13-15, 78-95)

4. Urząd dokonał nieprawidłowej anonimizacji trzech uchwał Rady Gminy Milejczyce Nr III/92/2019 z 31 grudnia 2019 r.; Nr IV/48/2019 z 27 marca 2019 r. oraz Nr IX/107/2020 z 31 marca 2020 r. umożliwiając tym samym odczytanie danych osobowych (imię i nazwisko) osób fizycznych, co było niezgodne z art. 5 ust. 1 lit. c *RODO.*

Przyczyną niezachowania zasady minimalizowania danych osobowych określonej w art. 5 ust. 1 lit. c *ogólnego rozporządzenia o ochronie danych* była nieprawidłowa anonimizacja. Mimo, że dane osoby skarżącej przy wstępnej analizie dokumentu były niewidoczne, to po skopiowaniu ich i wklejeniu do edytora tekstu możliwe było ich odczytanie.
(akta kontroli str. 3-5, 13-15)

5. Wskazane przez NIK stany nieprawidłowe opisane powyżej w pkt 1 i 4 przyczyniły się do podjęcia przez Urząd działań mających na celu zapewnienia pełnej ochrony danych, w tym danych osobowych gromadzonych w formie elektronicznej. W okresie od marca do maja 2023 roku Urząd podjął następujące działania naprawcze:

- usunięto wszystkie adresy e-mail, z których korzystali w celach służbowych pracownicy Urzędu i jednostek organizacyjnych, zlokalizowanych na internetowych domenach komercyjnych, z którymi nie zawarto umów powierzenia przetwarzania danych osobowych;
- zmieniono główne adresy e-mail jednostek organizacyjnych UG Milejczyce: w Gminnym Ośrodku Pomocy Społecznej w Milejczycach – gops@ug.milejczyce.wrotapodlasia.pl, w Szkole Podstawowej w Milejczycach – szkola@ug.milejczyce.wrotapodlasia.pl;
- zanonimizowano uchwały, w których pierwotnie zastosowano nieprawidłową anonimizację;
- zaktualizowano – z inicjatywy Urzędu – porozumienie z Urzędem Marszałkowskim na prowadzenie BIP i poczty elektronicznej w domenie *wrotapodlasia.pl.*

Wójt Gminy wyjaśnił też, że podjęto działania *w zakresie ukierunkowania i wskazania kierunku działania jednostkom podległym w zakresie ochrony danych osobowych dotyczących m.in. poczty elektronicznej.* Wójt dodał, że *barierami dla efektywnej ochrony danych osobowych są głównie bariery kadrowe i finansowe. Natomiast w jednostkach podległych wykorzystywanie adresów poczty elektronicznej w domenach komercyjnych bez zawarcia stosownych umów powierzenia danych osobowych wynikało z nieświadomości zagrożeń (...).*
(akta kontroli str. 3-5, 6-7, 12-18, 19-154)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Brak skutecznej kontroli zarządczej w zakresie zawierania umów powierzenia przetwarzania danych osobowych przy powierzaniu przetwarzania danych, administrowanych przez gminne jednostki organizacyjne.
2. Opublikowanie – w trzech przypadkach – uchwał bez zastosowania prawidłowej anonimizacji danych osobowych osób fizycznych, w tym osób skarżących działalność organu lub kierownika podległej Urzędowi jednostki organizacyjnej.

Zdaniem NIK działania naprawcze wdrożone przez Urząd w okresie od lutego do maja 2023 roku opisane w pkt 5 wystąpienia pokontrolnego, w sekcji *Opis stanu faktycznego* spowodowały usunięcie wszystkich stwierdzonych w trakcie czynności kontrolnych nieprawidłowości.

IV. Wnioski

Wnioski

W związku ze stwierdzonymi nieprawidłowościami oraz podjętymi przez UG Milejczyce działaniami naprawczymi, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 *ustawy o NIK*, wnosi o:

1. Kontynuowanie działań w zakresie kontroli zarządczej na poziomie gminy, w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych, gromadzonych w formie elektronicznej, zarówno przez Urząd jak i gminne jednostki organizacyjne;
2. Rozważenie możliwości wyznaczenia jednego inspektora ochrony danych dla Urzędu i gminnych jednostek organizacyjnych, stosownie do art. 37 ust. 3 RODO.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK, kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK w Białymstoku. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań. W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Białystok, dnia 23 czerwca 2023 r.

Kontroler
Mariusz Lenkiewicz
doradca ekonomiczny

.....
podpis

p. o. DYREKTORA DELEGATURY
Najwyższej Izby Kontroli w Białymstoku
Janusz Pawelczyk

.....
podpis