NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.411.003.03.2023

Pan
Witold Łapiński
Wójt Gminy Poświętne
Urząd Gminy Poświętne
Poświętne 21, 18-112 Poświętne

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 Poświętne, Poświętne 21, 18-112 Poświętne[1]
Kierownik jednostki kontrolowanej	Witold Łapiński, Wójt Gminy Poświętne[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/45/2023 z 23 lutego 2023 r. (akta kontroli str. 1-2)

[1] Dalej: Urząd lub UG Poświętne.
[2] Pełniący funkcję od 1990 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 nie prowadził w pełni skutecznych działań, które gwarantowałyby odpowiedni poziom bezpieczeństwa danych, w tym danych osobowych gromadzonych przez Urząd w formie elektronicznej oraz nie realizował skutecznej i adekwatnej kontroli zarządczej w tym zakresie na poziomie jednostki samorządu terytorialnego (gminy).

W Urzędzie i w dwóch[5] (z czterech) gminnych jednostkach organizacyjnych gromadzono – w latach 2018-2022 – pocztę elektroniczną zawierającą dane osobowe z wykorzystaniem usługi hostingu na komercyjnych domenach internetowych. Odbywało się to bez zawarcia wymaganej umowy powierzenia przetwarzania danych osobowych z podmiotem przetwarzającym stosownie do wymogów 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]. Na niewystarczający stopień bezpieczeństwa przetwarzanych w Urzędzie danych osobowych wpływ miało również gromadzenie i upublicznianie na stronie internetowej Biuletynu Informacji Publicznej danych osobowych w oświadczeniach majątkowych po upływie czasu określonego w *ustawie z dnia 8 marca 1990 r. o samorządzie gminnym*[7]. Ponadto transmitowanie i upublicznianie przez Urząd sesji organu uchwałodawczego odbywało się bez przeprowadzenia wymaganej przepisami *RODO* analizy ryzyka wynikającego z korzystania z zewnętrznego serwisu internetowego podczas przetwarzania danych osobowych uczestników sesji Rady Gminy oraz bez transkrypcji wymaganej od 23 września 2020 r. przepisami prawa dotyczącymi dostępności cyfrowej[8].

Już w trakcie kontroli NIK – od lutego do maja 2023 r. – Urząd podjął szereg działań naprawczych celem zapewnienia pełnej ochrony danych będących przedmiotem niniejszej kontroli. W ich konsekwencji nieprawidłowości stwierdzone w zakresie przetwarzania danych osobowych na stronach internetowych i poczcie elektronicznej oraz w związku z odbywającymi się sesjami organu stanowiącego zostały usunięte zarówno w Urzędzie jak i podległych mu 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 Poświętne wykorzystywało dwa główne adresy mailowe poswietne@data.pl i sekretariat@ug.poswietne.wrotapodlasia.pl, z których pierwszy założony został około 2000 roku (pracownicy Urzędu nie znali dokładnej daty), a drugi około 2008 roku (pracownicy Urzędu nie znali dokładnej daty). W przypadku tego pierwszego adresu poczty internetowej, Urząd nie zawarł umowy powierzenia przetwarzania danych osobowych, mimo, że przetwarzano na tej skrzynce pocztowej dane osobowe, tj. imię, nazwisko, adres, co stanowiło naruszenie art. 28 ust. 3 RODO. Pracownicy Urzędu korzystali z imiennych skrzynek e-mailowych w domenie *@ug.poswietne.wrotapodlasia.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 Poświętnem i Gminnej Bibliotece Publicznej w Poświętnem.

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

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

[8] 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*.

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) podległe 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 wymaganej art. 28 ust. 3 RODO[9]. Na wszystkich głównych skrzynkach mailowych jednostek organizacyjnych przetwarzano głównie dane osobowe zwykłe, przede wszystkim imię, nazwisko, adres. 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, pracownicy instytucji samorządowych, innych instytucji publicznych (np. ministerstw), kontrahenci zewnętrzni oraz klienci podmiotu (np. osoby korzystające ze świadczeń społecznych w przypadku Gminnego Ośrodka Pomocy Społecznej w Poświętnem).

Jak wyjaśnił Wójt przyczynami stwierdzonych nieprawidłowości dotyczących użytkowania w Urzędzie i w podległych Urzędowi jednostkach organizacyjnych skrzynek mailowych na domenach komercyjnych bez zawarcia stosownych umów powierzenia przetwarzania danych osobowych były, m.in.: *niedopatrzenie w kwestii zawarcia umowy powierzenia przetwarzania danych osobowych* oraz *nieświadomość zagrożeń.*

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 Poświętne 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. 3-28, 29-39)

---

[9] W Gminnym Ośrodku Pomocy Społecznej w Poświętnem użytkowano adresu mailowego gops.poswietne@gmail.com i Gminnej Bibliotece Publicznej w Poświętnem – gbp.poswietne@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)

2. Na stronie internetowej http://bip.ug.poswietne.wrotapodlasia.pl/ UG Poświętne prowadził Biuletyn Informacji Publicznej (BIP) i zawarł 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 gminnym, które stosownie do art. 24h ust. 6 tej ustawy, przechowuje się przez okres sześciu lat. Pomimo tego w BIP Urzędu przechowywano oświadczenia majątkowe zawierające dane osobowe przez dłuższy okres, co było niezgodne zarówno z treścią art. 24h ust. 6 ustawy o samorządzie gminnym, jak też z zasadą minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c *RODO*. Stwierdzono bowiem, że w BIP Urzędu udostępniano 64 oświadczeń majątkowych, dla których minął termin przechowywania (retencji danych), a najstarsze z nich złożone były m.in. przez radnych i osoby zajmujące kierownicze stanowiska za 2015 rok.

Wójt wyjaśnił, że przyczyną nieprawidłowego udostępniania oświadczeń majątkowych zawierających m.in. dane osobowe osób zobowiązanych do ich złożenia było *niedopatrzenie.*
(akta kontroli str. 3-6, 11-28)

3. Do realizowania obowiązku publikacji sesji organu uchwałodawczego wynikającego z art. 20 ust. 1b ustawy o samorządzie gminnym Urząd – do dnia rozpoczęcia kontroli NIK – wykorzystywał kanał w powszechnie dostępnym serwisie *YouTube.* W Urzędzie nie przeprowadzono analizy ryzyka (oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych) wynikającej z korzystania podczas przetwarzania danych osobowych uczestników sesji Rady Gminy z tego narzędzia stosownie do wymogów art. 5 ust. 1 lit. f) w zw. z art. 5 ust. 2 oraz art. 24 *ogólnego rozporządzenia o ochronie danych.* W konsekwencji nie zawarto umowy powierzenia przetwarzania danych z jego właścicielem, o której mowa w art. 28 ust. 3 w zw. z art. 5 ust. 1 lit a oraz lit f *RODO*. Upubliczniane w serwisie *Youtube* sesje Rady Gminy nie zawierały ponadto wymaganej transkrypcji, co było niezgodne z wymogiem dostępności cyfrowej (od 23 września 2020 r.) określonym w *ustawie o dostępności stron internetowych.*

Wójt wyjaśnił, że przyczyną nieprawidłowości były *obiektywne przesłanki wynikające z konieczności racjonalnego gospodarowania wydatkami budżetowymi. W czasie wejścia w życie przepisów nakazujących nagrywanie i transmitowanie obrad sesji organów uchwałodawczych oferty firm oferujących nagrywanie i przechowywanie materiałów wiązały się ze znacznymi kosztami. Urząd w 2019 r. wydatkował na dostosowanie się do zmian w przepisach ok. 14 000 zł (m.in. na zakup sprzętu komputerowego, zakup oprogramowania i sprzętu do nagrywania, zakup oprogramowania i sprzętu do głosowania) . Z uwagi na chęć zaoszczędzenia wydatków został wybrany do tego celu serwis YouTube, który był bezpłatny.* Wójt dodał, że Urząd *jest na etapie rozpoznania ofert na rynku odnośnie transmitowania i nagrywania sesji Rady Gminy, zgodnie z wymogami RODO. (...) Jesteśmy umówieni z właścicielem portalu (...) na próbną transmisję po której, jeżeli spełni nasze oczekiwania podpiszemy umowę.* W zakresie obowiązkowej transkrypcji transmisji sesji rady gminy Wójt wyjaśnił, że *wymóg transkrypcji z sesji rady gminy zostanie spełniony poprzez podpisanie umowy z podmiotem zewnętrznym realizującym takie usługi. Umowa zostanie zawarta niezwłocznie po zawarciu umowy na transmitowanie i upublicznianie sesji rady gminy.*
(akta kontroli str. 3-6, 11-28)

4. W Urzędzie nie stwierdzono przypadków niezachowania zasady minimalizowania danych osobowych określonej w art. 5 ust. 1 lit. c *ogólnego rozporządzenia o ochronie danych* w stosunku do osób fizycznych, których dane osobowe występowałyby w uchwałach lub uzasadnieniach uchwał podejmowanych przez organ stanowiący.(akta kontroli str. 3-6, 11-28)

5. Wskazane przez NIK stany nieprawidłowe opisane powyżej w pkt 1-2 przyczyniły się do podjęcia przez Urząd działań mających na celu zapewnienie pełnej ochrony danych, w tym danych osobowych gromadzonych w formie elektronicznej. W okresie od lutego 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, w Gminnym Ośrodku Pomocy Społecznej w Poświętnem – gops@ug.poswietne.wrotapodlasia.pl, a w Gminnej Bibliotece Publicznej w Poświętnem – gbp@ug.poswietne.wrotapodlasia.pl;

– usunięto z BIP UG Poświętne oświadczenia majątkowe za lata 2013-2015 członków Zarządu i skarbnika, osób wydających decyzje administracyjne w imieniu Wójta, kierowników jednostek organizacyjnych i radnych;

– zawarto umowę główną i umowę powierzenia przetwarzania danych osobowych na transmitowanie i upublicznianie sesji Rady Gminy zgodnie z wymogami *RODO;*

– zawarto umowę powierzenia przetwarzania danych osobowych z podmiotem udostępniającym hosting i domenę *data.pl* (dla adresu mailowego poswietne@data.pl);

– zawarto umowę na transkrypcję treści z posiedzeń organu uchwałodawczego;

Wójt wyjaśnił, że *głównymi barierami dla efektywnej ochrony danych osobowych przechowywanych w formie elektronicznej są bariery finansowe i organizacyjne. Duża część obowiązków nałożonych na jst (między coroczne audyty KRI, transmitowanie, upublicznianie i transkrypcja sesji z posiedzeń rady gminy) wiąże się z koniecznością wydatkowania kolejnych środków finansowych. Gmina Poświętne dysponuje niewielkim budżetem. Ogromną część dochodów budżetowych pochłaniają kosztowne inwestycje, tj. przebudowa dróg lokalnych czy modernizacja sieci wodociągowej i kanalizacyjnej, które przyczyniają się do zwiększenia komfortu życia mieszkańców. Pozostałą część budżetu gmina przeznacza na tzw. Wydatki bieżące. Na skutek zauważalnej, zwłaszcza w ostatnich latach, wzrostowej tendencji cen energii elektrycznej, paliwa, podstawowych materiałów, a co za tym idzie świadczonych przez rynek usług, wydatki jakie gmina może przeznaczać na pokrycie bieżących kosztów administracyjnych są bardzo ograniczone. Stąd też wynika niekiedy konieczność „odkładania" poszczególnych wydatków w czasie.* Wójt dodał, że *Część nieprawidłowości wynika z dużego obciążenia pracowników bieżącymi obowiązkami. W Urzędzie zatrudnionych jest tylko 19 osób. Każdy z pracowników realizuje bardzo szeroki zakres obowiązków, z tego powodu niektóre działania podejmowane są z opóźnieniem.* Jak dodał Wójt *ma też świadomość, iż część z ujawnionych nieprawidłowości wynikała z braku świadomości o istniejącym niebezpieczeństwie. W przyszłości planuję więc podjąć działania mające na celu zniesienie bariery nieświadomości zagrożeń poprzez zwiększenie liczby szkoleń dla pracowników UG Poświętne i jednostek podległych.* Wójt poinformował w trakcie kontroli NIK, że *zobowiązał również kierowników jednostek podległych do zwrócenia większej uwagi na problemy związane z ochroną danych osobowych. Kierownicy zostali poinformowani, że główną domeną za pomocą której mogą prowadzić korespondencję elektroniczną jest domena wrotapodlasia.pl.* (akta kontroli str. 3-6, 7-8, 11-28, 40-70)

Stwierdzone nieprawidłowości

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

1. Powierzanie w latach 2018-2022 przetwarzania danych osobowych, administrowanych przez Urząd, właścicielom komercyjnych serwisów internetowych świadczących usługi bezpłatnej poczty e-mailowej bez zawarcia umowy powierzenia przetwarzania danych osobowych oraz brak kontroli zarządczej w zakresie zawierania takich umów przy powierzaniu przetwarzania danych, administrowanych przez gminne jednostki organizacyjne.

2. Opublikowanie w BIP 64 oświadczeń majątkowych, dla których minął sześcioletni okres przechowywania (retencji danych).

3. Powierzenie przetwarzania danych osobowych osób uczestniczących w sesjach Rady Gminy bez przeprowadzenia odpowiedniej analizy ryzyk i bez zawarcia umowy powierzenia przetwarzania danych osobowych.

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 Poświętne 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