NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.411.003.04.2023

Pan
Mariusz Korzeniewski
Wójt Gminy Wyszki
Urząd Gminy Wyszki
Piórkowska 2, 17-132 Wyszki

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 Wyszki, Piórkowska 2, 17-132 Wyszki[1]
Kierownik jednostki kontrolowanej	Mariusz Korzeniewski, Wójt Gminy Wyszki[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/46/2023 z 23 lutego 2023 r. (akta kontroli str. 1-2)

[1] Dalej: Urząd lub UG Wyszki.
[2] Pełniący funkcję od 8 grudnia 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 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 wykorzystywano w sposób zgodny z przepisami pocztę mailową do przechowywania i przetwarzania danych, w tym danych osobowych. W dwóch[5] (z czterech) gminnych jednostkach organizacyjnych stwierdzono jednak wieloletnie gromadzenie poczty elektronicznej zawierającej 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]. Transmitowanie i upublicznianie przez Urząd sesji organu uchwałodawczego odbywało się bez: [1] przeprowadzenia wymaganej przepisami *RODO* analizy ryzyka wynikającego z korzystania z zewnętrznego serwisu internetowego podczas przetwarzania danych osobowych uczestników sesji Rady Gminy; [2] transkrypcji wymaganej od 23 września 2020 r. przepisami prawa dotyczącymi dostępności cyfrowej[7]. Ponadto stwierdzono jeden przypadek gromadzenia i upubliczniania danych osobowych w oświadczeniu majątkowym na stronie internetowej Biuletynu Informacji Publicznej po upływie czasu określonego w *ustawie z dnia 8 marca 1990 r. o samorządzie gminnym*[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 wszystkie stany nieprawidłowe stwierdzone w zakresie przetwarzania danych osobowych na stronach internetowych i poczcie elektronicznej oraz w związku z odbywającymi się sesjami organu uchwałodawczego 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 Wyszki wykorzystywał główny adres mailowy *ug_wyszki@post.pl* w ramach zakupionych usług hostingowych, w których oprócz poczty elektronicznej obsługiwana jest strona internetowa Urzędu oraz domena internetowa. Na poczcie elektronicznej przetwarzano dane osobowe, tj. dane pracowników, dane o klientach i kontrahentach, imię i nazwisko, NIP, PESEL, adres zamieszkania, adres korespondencyjny, nr rachunku bankowego, datę urodzenia, fotografię, adres IP, adres e mail, czy numer telefonu. Kategoriami osób, których dane osobowe były przetwarzane przez Urząd byli pracownicy podmiotu, innych jednostek publicznych, kontrahenci oraz klienci podmiotu.

---

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

[5] W Gminnym Ośrodku Pomocy Społecznej w Wyszkach i Szkoła Podstawowej im. Księdza Franciszka Jakuba Falkowskiego w Topczewie.

[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*.

Zgodnie z wymogami art. 28 ust. 3 rozporządzenia RODO Urząd zawarł z dostawcą ww. usług umowę powierzenia przetwarzania danych osobowych.

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) 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 tych jednostek organizacyjnych przetwarzano dane osobowe zwykłe, przede wszystkim: imię i nazwisko, adres zamieszkania, adres email, numer telefonu, numer PESEL. 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 podmiotu, pracownicy innych instytucji publicznych, klienci podmiotu. W jednej jednostce podległej 18 pracowników użytkowało do celów służbowych adresy poczty elektronicznej założone przez siebie na komercyjnych domenach internetowych.

Jak wyjaśnił Wójt *przyczynami zaistniałej sytuacji – tj. posiadania przez niektóre jednostki organizacyjne tzw. kont pocztowych przeznaczonych do użytku prywatnego był brak dostatecznej świadomości co do zagrożeń wynikających z tego stanu rzeczy oraz możliwość korzystania z nieodpłatnych rozwiązań.*

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. W Urzędzie 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. 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 trzy z czterech jednostek organizacyjnych Gminy Wyszki 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. 3-23)

---

[9] W Gminnym Ośrodku Pomocy Społecznej w Wyszkach użytkowano pocztę mailową gopswyszki1@op.pl i Szkole Podstawowej im. Księdza Franciszka Jakuba Falkowskiego w Topczewie – sptopczewo@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 https://ugwyszki-bip.podlaskie.pl/ UG Wyszki 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. Poza jednym stwierdzonym przypadkiem[13], w BIP Urzędu przechowywano oświadczenia majątkowe zawierające dane osobowe zgodnie 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*.

Wójt wyjaśnił, że przyczyną nieprawidłowego udostępniania oświadczeń majątkowych zawierających m.in. dane osobowe osób zobowiązanych do ich złożenia było *niedopatrzenie oraz błędna interpretacji przepisów prawa.* (akta kontroli str. 3-6, 11-23, 108-112)

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.*

Na potrzebę zmiany serwisu zwracał uwagę inspektor ochrony danych, który w raporcie[14] sporządzonym w październiku 2022 roku stwierdził nieakceptowalną wartość ryzyka i potrzebę wdrożenia działań naprawczych w tym zakresie. W raporcie w *opisie ryzyka zidentyfikowanego jako średnie dla transmisji sesji rady gminy na YouTube* stwierdzono, *że żeby spełnić zasadę integralności i poufności, Urząd musi sporządzić umowę powierzenia przetwarzania danych osobowych, standardowe klauzule umowne. W chwili umieszczenia nagrania z sesji rady na YouTube to właśnie ta platforma staje się przedmiotem przetwarzającym. Aby przekazanie danych było legalne, konieczne jest więc zawarcie stosownej umowy powierzenia. Niestety Urząd jako użytkownik YouTube nieposiadający biznesowego konta Google nie ma takiej możliwości. (...) Innym zagrożeniem wynikającym z publikacji nagrań obrad rady na YouTube jest ryzyko umieszczenia wideo z sesji na serwerze, który znajduje się poza terenem Unii Europejskiej. (...) W tej sytuacji Urząd jako użytkownik platformy nie ma możliwości sprawdzenia, czy jego nagranie przechowywane jest na serwerze znajdującym się na terenie UE. W takim przypadku Urząd musi dopełnić kolejnych formalności w świetle RODO – w tym poinformować osoby z nagrania o ryzyku związanym z przekazywaniem ich danych osobowych poza Europejski Obszar Gospodarczy (EOG), czy uzyskać zgody od tych osób i to jeszcze zanim YouTube umieści dane na serwerze poza EOG.* W raporcie zwrócono też uwagę, że *Serwis ma prawo generowania przychodów z tytułu wszystkich zamieszczonych w nim treści. YouTube może więc bez zgody właściciela opublikowanego materiału wideo zdecydować o wyświetleniu w nim reklamy.* Jako działanie obniżające ryzyko do akceptowalnego poziomy zaproponowano w raporcie: *Rozwiązaniem problemu są usługi umieszczenia sesji online na serwerach znajdujących się na terenie Unii Europejskiej pozwalających na zgodność z RODO.*

Wójt wyjaśnił, że *Przyczyną takiego stanu rzeczy, tj. korzystania z YouTube była niejednoznaczność stanowisk, co do możliwości korzystania z tego serwisu przez Gminy, jak też możliwość prowadzenia transmisji obrad bez ponoszenia dodatkowych kosztów przez Gminę. (...) IOD przeprowadził analizę ryzyka dotyczącą transmisji i upubliczniania sesji, w wyniku której zalecił wprowadzenie stosowanych zmian pozwalających w szczególności na zapewnieniu dostawcy umożliwiającego zawarcie umowy powierzenia przetwarzania danych osobowych (analiza ryzyka z dnia 28.10.2022 r). Wskazano w niej, iż rozwiązaniem problemu*

---

[13] Oświadczenie Wójta za 2014 rok.

[14] Jednolita analizie kontrolna krajowych ram operacyjności sporządzona 28 października 2022 r.

są usługi umieszczania sesji online na serwerach znajdujących się na terenie Unii Europejskiej pozwalających na zgodność z RODO (...). Na tej podstawie oraz w wyniku przeprowadzanej kontroli dokonano zmian. (akta kontroli str. 3-6, 12-23, 66-81)

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)

5. Wskazane przez NIK stany nieprawidłowe opisane powyżej w pkt 1-3 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 lutego do maja 2023 roku Urząd podjął następujące działania naprawcze:

- usunięto wszystkie adresy e-mail, z których korzystali w celach służbowych pracownicy jednostek organizacyjnych, zlokalizowanych na internetowych domenach komercyjnych, z którymi nie zawarto umów powierzenia przetwarzania danych osobowych;
- zmieniono główne adresy e-mail gminnych jednostek organizacyjnych: w Szkole Podstawowej im. księdza Franciszka Jakuba Falkowskiego w Topczewie – sptopczewo@wyszki.pl; w Gminnym Ośrodku Pomocy Społecznej w Wyszkach – gops@wyszki.pl;
- usunięto z BIP Urzędu jedno oświadczenie majątkowe z 2014 roku;
- nawiązano umowę na transkrypcję sesji organu stanowiącego.

Wójt wyjaśnił ponadto, że *Urząd na skutek kontroli zmienił sposób transmitowania sesji organu uchwałodawczego gminy, zawarł umowę z dostawcą oprogramowania proponowanego gminom. Poza tym inspektor ochrony danych planuje przeprowadzenie dodatkowego szkolenia w celu podniesienia świadomości osób przetwarzających dane osobowe. Zidentyfikowanymi barierami, jeżeli chodzi o procesy przetwarzania danych osobowych są finanse, oraz często zbyt wiele różnych obowiązków nałożonych na pracowników (konieczność zajmowania się różnymi rodzajami spraw spowodowana specyfiką małej gminy). Stąd – skrzynki pocztowe zostały założone przy wykorzystaniu infrastruktury Urzędu.*
(akta kontroli str. 3-6, 7-8, 12-23, 24-40, 82-107, 108-112)

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 BIP jednego oświadczenia majątkowego, dla którego 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 Wyszki działaniami naprawczymi, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 *ustawy o NIK*, wnosi o 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;

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