NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.411.003.10.2023

Pan
Kazimierz Ramotowski
Wójt Gminy Przytuły
Urząd Gminy Przytuły
ul. Supska 10, 18-423 Przytuły

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 Przytuły, ul. Supska 10, 18-423 Przytuły[1]
Kierownik jednostki kontrolowanej	Kazimierz Ramotowski, Wójt Gminy Przytuły[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	Wojciech Zambrzycki, doradca ekonomiczny, upoważnienie do kontroli nr LBI/53/2023 z 2 marca 2023 r. (akta kontroli str. 1-2)

[1] Dalej: Urząd.
[2] Od 1 maja 2010 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 we wszystkich czterech[5] gminnych jednostkach organizacyjnych gromadzono – w latach 2018-2022 – pocztę elektroniczną zawierającą dane osobowe z wykorzystaniem usługi hostingu na komercyjnych domenach internetowych 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]. Na niewystarczający stopień bezpieczeństwa przetwarzanych w Urzędzie danych osobowych wpływ miało także gromadzenie i upublicznianie na stronie internetowej Biuletynu Informacji Publicznej[7] danych osobowych w oświadczeniach majątkowych po upływie czasu określonego w art. 24h ust. 6 *ustawy z dnia 8 marca 1990 r. o samorządzie gminnym*[8]. Ponadto transmitowanie i upublicznianie przez Urząd sesji organu uchwałodawczego odbywało się bez: [1] przeprowadzenia wymaganej przepisami *RODO* analizy ryzyka, wynikającej z wykorzystania serwisu *YouTube* podczas przetwarzania danych osobowych uczestników sesji Rady Miejskiej oraz [2] transkrypcji wymaganej od 23 września 2020 r. przepisami prawa dotyczącymi dostępności cyfrowej[9].

Jednak już w trakcie kontroli NIK – od lutego do maja 2023 roku – Urząd podjął działania naprawcze celem zapewnienia pełnej ochrony danych będących przedmiotem niniejszej kontroli. W ich konsekwencji większość nieprawidłowości w zakresie ochrony i przetwarzania danych osobowych na stronach internetowych, poczcie elektronicznej oraz transmisji sesji Rady Gminy zostało usuniętych zarówno w Urzędzie, jak i gminnych jednostkach organizacyjnych, lub zaplanowano ich usunięcie.

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

1. Urząd korzystał z poczty elektronicznej pod adresem gmina@przytuly.powiatlomzynski.pl którą utworzył w 2006 roku. Pracownicy Urzędu również korzystali ze skrzynek e-mailowych w tej domenie. Z hostingodawcą Urząd miał zawartą umowę powierzenia przetwarzania danych, o której mowa w art. 28 ust. 3 *RODO*[10].

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.

---

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

[5] W Ośrodku Pomocy Społecznej w Przytułach, Gminnej Bibliotece Publicznej, Szkole Podstawowej w Przytułach i Szkole Podstawowej w Wagach.

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

[7] Dalej: BIP

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

[9] 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*.

[10] 1 września 2018 r.

Gminny Ośrodek Pomocy Społecznej w okresie objętym kontrolą korzystał ze skrzynki e-mailowej pod adresem gopsprzytuly@wp.pl założonej na osobę fizyczną. Na skrzynce e-mailowej znajdowała się korespondencja związana z załatwianiem spraw bieżących dotyczących funkcjonowania GOPS i z zakresu zadań własnych gminy w sprawach pomocy społecznej. Korespondencja była prowadzona wewnątrz Gminy Przytuły oraz z innymi instytucjami publicznymi (w tym. Regionalnym Ośrodkiem Pomocy Społecznej, ośrodkami pomocy społecznej, Podlaskim Urzędem Wojewódzkim) i osobami fizycznymi. Wysyłane i odbierane były wiadomości zawierające dane osobowe osób fizycznych, dane o ich stanie zdrowia, o korzystaniu ze świadczeń opieki społecznej (imiona, nazwiska, adresy, numery PESEL, dane o zatrudnieniu i wysokości wynagrodzenia, dane o sytuacji rodzinnej). Do czasu rozpoczęcia kontroli NIK, z właścicielem domeny nie zawarto umowa powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*.

Szkoła Podstawowa w Przytułach w okresie objętym kontrolą korzystała z bezpłatnej skrzynki e-mailowej przytuly.szkola@gmail.com, założonej na osobę fizyczną[11]. Na poczcie internetowej w tym serwisie znajdowała się korespondencja związana z załatwianiem bieżących spraw dotyczących funkcjonowania szkoły oraz z zakresu zadań własnych gminy w sprawach edukacji publicznej. Korespondencja była prowadzona zarówno wewnątrz Gminy Przytuły jak też z innymi instytucjami publicznymi (m.in. Głównym Urzędem Statystycznym, Ministerstwem Edukacji, Kuratorium Oświaty). Przed przeprowadzonymi oględzinami NIK większość wiadomości ze skrzynki e-mailowej została skasowana[12], w pozostałych wiadomościach znajdowały się imiona i nazwiska osób fizycznych. Z właścicielem domeny nie zawarto umowy powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*.

Biblioteka Publiczna w Przytułach korzystała ze skrzynki e-mailowej biblioteka_przytuly@wp.pl założonej dla osoby fizycznej. Na skrzynce e-mailowej znajdowała się korespondencja związana z załatwianiem bieżących spraw, w tym m.in. faktury zakupowe, oferty handlowe, nowości wydawnicze, korespondencja wewnątrz Gminy Przytuły oraz z urzędami centralnymi. Nie stwierdzono wiadomości zawierających dane osobowe osób fizycznych. Z właścicielem domeny nie była zawarta umowa powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*.

(akta kontroli str. 3-21, 46-47)

Wójt wyjaśnił, że skrzynki e-mailowych na portalach komercyjnych były darmowe oraz funkcjonowały bardzo długo w świadomości klientów jednostek podległych, dlatego też te jednostki korzystały z tych adresów e-mailowych, chociaż bez zawartej umowy powierzenia przetwarzania danych z procesorem. Wójt widzi również bariery takie jak finansowa (brak środków w budżecie na zakup infrastruktury informatycznej), kadrowa (mało osób chętnych do pracy w małych urzędach) oraz barierę w dostępie do wiedzy (drogie szkolenia) – które przyczyniają się do nieefektywnej ochrony danych osobowych. (akta kontroli str. 33, 142)

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*[13] wszystkie gminne jednostki organizacyjne jako podmioty sektora finansów publicznych są samodzielnymi administratorami danych. 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*.

---

[11] W Szkole Podstawowej w Wagach odstąpiono od oględzin skrzynki e-mailowej pod adresem wagi4@wp.pl.

[12] Według oświadczenia kierownika placówki.

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

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*[14] i do części I.2.3 – I.2.6 *Standardów kontroli zarządczej dla sektora finansów publicznych*[15] – aby umowy takie zawarte zostały przez wszystkie gminne jednostki organizacyjne.

NIK zwraca też uwagę, że trzy z czterech jednostek organizacyjnych Gminy Przytuły funkcjonują 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. Brak ścisłego nadzoru nad jednostkami podległymi w tym zakresie oraz użytkowanie w celach służbowych kont pocztowych zakładanych w domenach komercyjnych bez skutecznych instrumentów zapewniających odpowiedni poziom bezpieczeństwa dla przetwarzanych danych osobowych NIK podnosiła już wielokrotnie w swoich kontrolach.

W trakcie kontroli NIK jednostkom podległym założono adresy e-mailowe w domenie @przytuly.powiatlomzynski.pl i zaprzestano korzystać ze skrzynek w domenach komercyjnych, a 21 kwietnia 2023 r. pracowników Urzędu przeszkolono z podstaw cyberprzestępczości. Ponadto podjęto inne działania: wyłoniony podmiot zewnętrzny przejmie obowiązki Inspektora Ochrony Danych oraz przeprowadzi szkolenie w zakresie ochrony danych osobowych, a korzystając z możliwości wydatkowania grantu z projektu *Cyfrowa Gmina* zaplanowano audyt (szerzej o braku audytów w punkcie 5. niniejszego wystąpienia).

(akta kontroli str. 33, 46-47)

2. Urząd prowadził Biuletyn Informacji Publicznej na stronie internetowej https://www.przytuly.powiatlomzynski.pl/bip a z właścicielem tego serwisu miał zawartą umowę powierzenia przetwarzania danych osobowych[16]. W BIP publikowane były m.in. oświadczenia majątkowe osób, o których mowa w art. 24h ust. 1 *ustawy o samorządzie gminnym*, przy czym 70 (z 190, tj. 37%) przechowywano ponad sześć lat, najstarsze złożone były za 2003 rok. Było to niezgodne zarówno z art. 24h ust. 6 *usg*, określającym, że oświadczenia te przechowuje się przez sześć lat, jak też z zasadą minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c *RODO*. Wójt wyjaśnił, że powodem publikacji oświadczeń po terminie retencji danych było przeoczenie obowiązku ich usunięcia oraz rozproszenie na rożnych podstronach BIP.

Oświadczenia majątkowe które były opublikowane w BIP w dniu rozpoczęcia kontroli[17], a dla których minął okres retencji danych, zostały z BIP usunięte 13 marca 2023 r.

(akta kontroli str. 22-23, 142)

3. Do realizowania obowiązku publikacji odbywających się sesji organów uchwałodawczych – o czym mowa w art. 20 ust. 1b *ustawy o samorządzie gminnym* – Urząd wykorzystywał portal *YouTube* na którym opublikował 25 nagrań z sesji Rady Gminy w kadencji 2018-2023[18]. W przypadku tego serwisu, wbrew przepisom art. 5 ust. 1 lit. f) w zw. z art. 5 ust. 2 oraz art. 24 *ogólnego rozporządzenia o ochronie danych* 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.*

---

[14] Dz. U. z 2022 r. poz. 1634, ze zm.
[15] Ogłoszonych Komunikatem Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. (Dz. Urz. MF Nr 15, poz. 84).
[16] 1 września 2018 r.
[17] 3 marca 2023 r.
[18] Nie miał opublikowanych obrad z poprzedniej kadencji, brak odnośników w BIP.

Wójt wyjaśnił również, że informatyk Urzędu przeprowadził czynności wyłaniające nowego operatora sesji Rady Gminy, który podejmie się również przeniesienia (do końca czerwca 2023 r.) nagrań sesji Rady Gminy z serwisu *YouTube* na portal esesja.tv.

(akta kontroli str. 24, 33, 42)

4. Przedmiotem analizy NIK było również zweryfikowanie, czy w przypadku skarg na Wójta Gminy i/lub kierowników jednostek mu podległych, opublikowane uchwały były właściwie zanonimizowane. W przypadku dwóch takich skarg[19] nie stwierdzono ujawnienia danych osób wnoszących skargi. (akta kontroli str. 25)

5. Zarówno w Urzędzie jak też podległych jednostkach w latach 2018-2022 nie był przeprowadzony coroczny audyt wewnętrzny w zakresie bezpieczeństwa informacji, do czego kierownictwo podmiotów publicznych zobowiązane było na mocy § 20 ust. 2 pkt 14 *rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[20]. W związku z realizacją projektu *Cyfrowa Gmina* audyt przeprowadzony ma być w 2023 roku. Przyczyną nieprzeprowadzania audytów była niewiedza oraz brak środków finansowych na takie działanie – wyjaśnił Wójt. Zdaniem NIK właściwie przeprowadzony audyt wewnętrzny powinien ujawnić stany nieprawidłowe opisane w niniejszym wystąpieniu pokontrolnym.

(akta kontroli str. 32, 142)

Stwierdzone nieprawidłowości

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

1. Powierzenie w latach 2018-2022 przetwarzania danych osobowych, 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. Publikowanie w BIP 70 oświadczeń majątkowych, dla których minął sześcioletni okres przechowywania (retencji danych).
3. Powierzenie danych w postaci wizerunku osób uczestniczących w 25 sesjach Rady Gminy Przytuły właścicielowi serwisu *YouTube* bez przeprowadzenia odpowiedniej analizy ryzyk i bez zawarcia umowy powierzenia przetwarzania danych osobowych.
4. Nieprzeprowadzanie corocznych audytów wewnętrznych w zakresie bezpieczeństwa informacji.

Zdaniem NIK działania naprawcze wdrożone przez Urząd w okresie od lutego do maja 2023 roku opisane w pkt 1-3 wystąpienia pokontrolnego, w sekcji *Opis stanu faktycznego* doprowadziły do usunięcia nieprawidłowości stwierdzonych w p-ktach 1-3, lub zaplanowano ich usunięcie.

IV. Uwagi i wnioski

Uwagi i wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 *ustawy o NIK*, wnosi o:

1. Usunięcie materiałów video z nagraniami obrad sesji rady gminy z serwisu *YouTube* lub zawarcie umowy powierzenia przetwarzania danych z jego właścicielem.
2. 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.

Z uwagi na działania podjęte przez Urząd, Najwyższa Izba Kontroli odstępuje od formułowania wniosków pokontrolnych w pozostałym zakresie.

---

[19] Rozpatrywanych w uchwałach: VII/48/2019 i VIII/53/2019,

[20] Dz. U. z 2017 poz. 2247.

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 wykonania wniosków

Zgodnie z art. 62 *ustawy o NIK*, należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie 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

Wojciech Zambrzycki
doradca ekonomiczny

.....
podpis

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

.....
podpis