NAJWYŻSZA IZBA KONTROLI

Delegatura w Białymstoku

LBI.411.003.05.2023

Pan
Kazimierz Górski
Wójt Gminy Miastkowo
Urząd Gminy Miastkowo
ul. Łomżyńska 32, 18-413 Miastkowo

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 Miastkowo, ul. Łomżyńska 32, 18-413 Miastkowo[1]
Kierownik jednostki kontrolowanej	Kazimierz Górski, Wójt Gminy Miastkowo[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/49/2023 z 23 lutego 2023 r. (akta kontroli str. 1-2)

[1] Dalej: Urząd.
[2] Od 24 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 jednostek organizacyjnych powiatu 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 (do 2020 roku) i we wszystkich pięciu[5] gminnych jednostkach organizacyjnych w latach 2018-2022 gromadzono 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 (BIP) danych osobowych w oświadczeniach majątkowych po upływie czasu określonego w art. 24h ust. 6 *ustawy z dnia 8 marca 1990 r. o samorządzie gminnym*[7]. Transmitowanie i upublicznianie przez Urząd części sesji organu uchwałodawczego odbywało się bez przeprowadzenia wymaganej analizy ryzyka wynikającej z korzystania z serwisu internetowego podczas przetwarzania danych osobowych uczestników sesji Rady Gminy.

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 nieprawidłowości w zakresie ochrony i przetwarzania danych osobowych na stronach internetowych, poczcie elektronicznej oraz transmisji sesji Rady Gminy 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

1. Urząd korzystał z poczty elektronicznej pod adresem gmina@miastkowo.pl, którą utworzył w 2020 roku, a wcześniej z adresu w domenie @gmail.com. Pracownicy Urzędu również korzystali ze skrzynek e-mailowych w tej domenie, do czasu zakupienia domeny @miastkowo.pl. Z właścicielem serwisu gmail.com Urząd nie miał zawartej umowy powierzenia przetwarzania danych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*.

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.

Gminny Ośrodek Pomocy Społecznej w okresie objętym kontrolą korzystał ze skrzynki e-mailowej pod adresem ops.miastkowo@gmail.com założonej na osobę fizyczną, a od września 2022 roku decyzją nowego kierownika również ze skrzynki ops@miastkowo.pl przy czym jednocześnie poprzednio używana nie została zamknięta. Na skrzynce e-mailowej w serwisie gmail.com znajdowała się korespondencja związana z załatwianiem spraw bieżących dotyczących funkcjonowania GOPS i z zakresu zadań własnych gminy w sprawach

---

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

[5] W Gminnym Ośrodku Pomocy Społecznej w Miastkowie, Gminnym Ośrodku Kultury w Miastkowie, Szkole Podstawowej w Miastkowie, Szkole Podstawowej w Rydzewie, Bibliotece Publicznej Gminy Miastkowie.

[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*.

pomocy społecznej. Korespondencja była prowadzona wewnątrz Gminy Miastkowo 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 była zawarta umowa powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*.

Szkoła Podstawowa w Miastkowie korzystała ze skrzynki e-mailowej miastkowo@gmail.com założonej w 2008 roku, jako skrzynka bezpłatna, założona na osobę fizyczną[8]. 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 Miastkowo, jak też z innymi instytucjami publicznymi (m.in. Główny Urząd Statystyczny, Ministerstwo Edukacji, Kuratorium Oświaty) oraz z nauczycielami (nauczyciele korzystali z prywatnych adresów e-mailowych). Wysyłane i odbierane były wiadomości zawierające m.in. dane osobowe osób fizycznych, takie jak: imiona, nazwiska (w tym uczniów szkoły), numery PESEL, adresy, numery telefonów. Z właścicielem domeny nie były zawarte umowy powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*.

W okresie objętym kontrolą Gminny Ośrodek Kultury korzystał ze skrzynki e-mailowej gokm@op.pl, jako skrzynki bezpłatnej założonej na osobę fizyczną. Na skrzynce e-mailowej znajdowała się korespondencja związana z załatwianiem bieżących spraw, w tym m.in. faktury zakupowe i oferty handlowe. Znajdowała się tam również korespondencja zawierająca dane osobowe, w tym m.in.: imiona, nazwiska, adresy e-mail, numery telefonów, numery PESEL uczestników projektów. Z właścicielem domeny nie była zawarta umowa powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*.

Biblioteka Publiczna Gminy Miastkowo korzystała ze skrzynki e-mailowej biblioteka-miastkowo@o2.pl założonej w 2005 roku, jako konto 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 Miastkowo oraz z urzędami centralnymi. Znajdowała się tam również korespondencja zawierająca dane osobowe, w tym imiona, nazwiska, adresy numery PESEL. Z właścicielem domeny nie była zawarta umowa powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*.

Wójt wyjaśnił, że to niewiedza była przyczyną korzystania ze skrzynek e-mailowych na portalach komercyjnych, bez zawartej umowy powierzenia przetwarzania danych z procesorem[9]. (akta kontroli str. 4-41, 45-49, 188-190)

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. 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

---

[8] W Szkole Podstawowej w Rydzewie odstąpiono od oględzin skrzynki e-mailowej pod adresem sprydzewo@wp.pl.

[9] Podmiot, który przetwarza dane w imieniu administratora.

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

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 pięciu jednostek organizacyjnych Gminy Miastkowo 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 (poza Ośrodkiem Pomocy Społecznej) założono adresy e-mailowe w domenie @miastokowo.pl (ośrodek już ją taką pocztę posiadał). Zaprzestano także korzystać ze skrzynek w domenach komercyjnych, 9 marca 2023 r. zorganizowano szkolenie z tematyki ochrony danych osobowych wszystkim pracownikom Urzędu, zawarto umowę z zewnętrznym podmiotem, który przeprowadzi analizę ryzyka oraz audyt w zakresie danych osobowych. (akta kontroli str. 48-49, 188-190)

2. Urząd prowadził Biuletyn Informacji Publicznej na stronie internetowej https://www.miastkowo.pl/bip. W BIP publikowane były m.in. oświadczenia majątkowe osób, o których mowa w art. 24h ust. 1 *ustawy o samorządzie gminnym*, przy czym 126 (z 312, tj. 40%) przechowywano ponad sześć lat, najstarsze złożone były za 2013 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.

Oświadczenia majątkowe, które były opublikowane w BIP w dniu rozpoczęcia kontroli[13], a dla których minął okres retencji danych, zostały z BIP usunięte 27 lutego 2023 r.

(akta kontroli str. 3, 48-49)

3. Do realizowania obowiązku publikacji odbywających się sesji organów uchwałodawczych – o czym mowa w art. 20 ust. 1b *ustawy o samorządzie gminnym* – Urząd wykorzystywał własny serwer, na którym umieszczał nagrania i transmitował obrady. Na próbie pięciu[14] (z 20 sesji) ustalono, że wywiązano się z obowiązku transkrypcji obrad, który nałożono od 23 września 2020 r. ma mocy załącznika do *ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych*[15] (napisy rozszerzone i audiodeskrypcja). (akta kontroli str. 192)

Jednocześnie Urząd Gminy opublikował na portalu *YouTube* 21 materiałów video (w tym trzy sesje obrad Rady Gminy z kadencji 2018-2023: III, IX i X). Wójt jako administrator danych osobowych wbrew przepisom art. 5 ust. 1 lit. f) w zw. z art. 5 ust. 2 oraz art. 24 *ogólnego rozporządzenia o ochronie danych* nie przeprowadził analizy ryzyka (oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych) wynikającej z korzystania podczas przetwarzania danych osobowych uczestników sesji Rady Miejskiej.

---

[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).

[13] 24 lutego 2023 r.

[14] Sesje nr: XXXIII, XXIX, XXV, XIX, XVII Rady Gminy.

[15] Dz. U. z 2023 r. poz. 82 ze zm.

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*. Wójt Gminy wyjaśnił, że powodem niezawarcia takiej umowy było to, że właściciel serwisu prowadzi jedynie politykę prywatności i wbudowane zaawansowane funkcje zabezpieczeń, które nieustannie chronią dane. Najwyższa Izba Kontroli zauważa jednak, że jest to przesłanka do odstąpienia od zawarcia stosownej umowy powierzenia przetwarzania danych.

Opublikowane filmy oraz profil Gminy Miastkowo został usunięty z serwisu *YouTube* w trakcie trwania kontroli NIK. (akta kontroli str. 48-49, 193-196)

4. W okresie objętym kontrolą Rada Gminy dwukrotnie obradowała nad skargami na działanie Wójta Gminy. Obie uchwały podjęte w tej sprawie (z 13 marca 2020 r. i 20 lutego 2023 r.) zostały właściwie zanonimizowane i w BIP nie opublikowano personaliów skarżących.
(akta kontroli str. 191)

5. Zarówno w Urzędzie, jak też podległych jednostkach w latach 2018-2022 na ogół 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*[16]. W okresie objętym kontrolą audyt ten przeprowadzono jedynie w Szkole Podstawowej w Rydzewie w 2022 roku oraz w Urzędzie Gminy w 2023 roku w związku z realizacją projektu *Cyfrowa Gmina*. Przyczyną nieprzeprowadzania audytów była niewiedza oraz nadmiar innych obowiązków – wyjaśnił Wójt. Zdaniem NIK właściwie przeprowadzony audyt wewnętrzny powinien ujawnić stany nieprawidłowe opisane w niniejszym wystąpieniu pokontrolnym.
(akta kontroli str. 48-49)

Stwierdzone nieprawidłowości

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

1. Powierzenie 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. Publikowanie w BIP 126 oświadczeń majątkowych, dla których minął sześcioletni okres przechowywania (retencji danych).
3. Powierzenie danych w postaci wizerunku na 21 materiałach video osób uczestniczących w trzech sesjach Rady Gminy Miastkowo i innych wydarzeniach z życia gminy, 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 wskazane w punktach 1-3 *Opisu ustalonego staniu faktycznego* doprowadziły do usunięcia nieprawidłowości stwierdzonych w p-ktach 1-3.

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: 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.

---

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

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

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