NAJWYŻSZA IZBA KONTROLI

Delegatura w Białymstoku

LBI.411.003.09.2023

Pan
Mariusz Soliwoda
Wójt Gminy Wizna
Urząd Gminy Wizna
Plac Kpt. Raginisa 35, 18-430 Wizna

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 Wizna, Plac Kpt. Raginisa 35, 18-430 Wizna[1]
Kierownik jednostki kontrolowanej	Mariusz Soliwoda, Wójt Gminy Wizna[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/70/2023 z 24 marca 2023 r. (akta kontroli str. 1-2)

[1] Dalej: Urząd.
[2] Od 21 października 2018 r., wcześniej tą funkcję w okresie objętym kontrolą pełnił Zbigniew Sokołowski.
[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 prowadził efektywne działania, które skutkowały odpowiednim poziomem bezpieczeństwa danych, w tym danych osobowych gromadzonych przez ten podmiot. Nie realizował jednak skutecznej i adekwatnej kontroli zarządczej w tym zakresie na poziomie jednostki samorządu terytorialnego (gminy).

Urząd zapewnił transmisję obrad sesji organu uchwałodawczego oraz zapewnił transkrypcję wymaganą od 23 września 2020 r. przepisami prawa dotyczącymi dostępności cyfrowej[5]. Na stronie Biuletynu Informacji Publicznej (BIP) publikował oświadczenia majątkowe i dbał o właściwą retencję danych, określoną w art. 24h ust. 6 *ustawy z dnia 8 marca 1990 r. o samorządzie gminnym*[6]. W publikacjach na BIP anonimizowano dane skarżących.

Jednakże w dwóch z czterech[7] 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*[8].

Już w trakcie kontroli NIK – od marca do maja 2023 roku – Urząd podjął działania naprawcze celem zapewnienia pełnej ochrony danych będących przedmiotem niniejszej kontroli.

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 sekretariat@gminawizna.pl, którą utworzył w 2018 roku (wcześniej zaś w domenie @wizna.pl). Pracownicy Urzędu korzystali z imiennych skrzynek e-mailowych w tej samej domenie. Z hostingodawcą zawarta była umowa powierzenia przetwarzania danych, na podstawie art. 28 ust. 3 *RODO*[9].

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 korzystał ze skrzynki e-mailowej pod adresem gops_wizna@wp.pl, była to skrzynka bezpłatna założona 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 Wizna 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

---

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

[5] 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*.

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

[7] W Gminnym Ośrodku Pomocy Społecznej w Wiźnie, Bibliotece Publicznej w Wiźnie.

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

[9] 13 grudnia 2019 r.

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 Wiźnie miała wykupioną własną domenę @spwizna.pl i wszyscy pracownicy szkoły dysponowali adresami e-mailowymi w tej domenie. Z hostingodawcą nie była zawarta umowa powierzenia przetwarzania danych osobowych, o której mowa w art. 28 ust. 3 *RODO*. Dyrektor szkoły ze skrzynki dyrektor@spwizna.pl wysyłała również wiadomości zawierające dane służbowe na swoją skrzynkę prywatną w domenie wp.pl.

Biblioteka i jej filia w Bronowie korzystały ze skrzynek poczty elektronicznej w domenie wp.pl (odpowiednio: biblioteka_wizna@wp.pl i bibliotekabronowo1@wp.pl)[10], chociaż utworzony i używany był również adres e-mailowy biblioteka@gminawizna.pl. Z właścicielem domeny wp.pl nie była zawarta umowa powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*. (akta kontroli str. 24-42,317)

Przyczyną korzystania ze skrzynek e-mailowych na portalach komercyjnych, bez zawartej umowy powierzenia przetwarzania danych z procesorem, był przede wszystkim brak świadomości kierownictwa tych jednostek o potrzebie zawarcia takiej umowy. Skrzynki e-mailowe Gminnego Ośrodka Pomocy Społecznej i Biblioteki w serwisie wp.pl zostały założone przed wejściem w życie przepisów rozporządzenia *RODO*. (akta kontroli str. 52, 55)

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*[11] 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*.

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*[12] i do części I.2.3 – I.2.6 *Standardów kontroli zarządczej dla sektora finansów publicznych*[13] – aby umowy takie zawarte zostały przez wszystkie gminne jednostki organizacyjne.

NIK zwraca też uwagę, że trzy z czterech jednostek organizacyjnych Gminy Wizna 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.

---

[10] Z uwagi na niskie ryzyko przetwarzania danych osobowych na skrzynkach e-mailowych bibliotek odstąpiono od oględzin ich zawartości.

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

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

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

W trakcie kontroli NIK pracowników Ośrodka Pomocy Społecznej oraz bibliotek zobowiązano do zaprzestania korzystania z domen e-mailowych, których serwery nie są znane, a mogą być zlokalizowane poza UE, a 7 marca 2023 r. założony został adres e-mailowy ops@gminawizna.pl. (akta kontroli str. 48)

2. Urząd prowadził Biuletyn Informacji Publicznej na stronie internetowej http://www.bip.wizna.pl/ a z właścicielem tego serwisu miał zawartą umowę powierzenia przetwarzania danych osobowych[14]. Żadne z opublikowanych oświadczeń majątkowych nie pozostawało poza sześcioletnim okresem retencji danych, o którym mowa w art. 24h ust. 1 *ustawy o samorządzie gminnym*. (akta kontroli str. 3)

3. Do realizowania obowiązku publikacji odbywających się sesji organów uchwałodawczych – o czym mowa w art. 20 ust. 1b *ustawy o samorządzie gminnym* – Urząd wykorzystywał od czerwca 2021 roku własny serwer, na którym umieszczał nagrania i transmitował obrady. Wcześniej nagrania przechowywane były na lokalnej stacji roboczej, a udostępnienie miało miejsce na stronie internetowej Urzędu jako pliki wtyczki Adobre Flash Player[15]. Na próbie pięciu[16] (z 20 sesji) ustalono, że wywiązano się z obowiązku transkrypcji obrad, który nałożono od 23 września 2020 r. ma mocy załącznika do *ustawy o dostępności stron internetowych*. (akta kontroli str. 4-6, 310-311)

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 23 takich skarg zanominizowano dane skarżących. Dwie z nich zawierały jednak sformułowania powszechnie uznane za obelżywe i tych zwrotów nie usunięto przy publikacji treści skargi, przy czym Wójt wyjaśnił, że przepisy *ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego*[17] oraz *rozporządzenia Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków*[18] nie zezwalają organowi na ingerencję w treść skargi. (akta kontroli str. 7-23, 311)

5. Stosownie do treści § 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*[19] kierownictwo podmiotów publicznych zobowiązane było przeprowadzać coroczny audyt wewnętrzny w zakresie bezpieczeństwa informacji. W Urzędzie audyt taki przeprowadzono w 2019 roku, a kolejny w 2022 roku. Przyczyną braku audytów w latach 2020-2021, jak wyjaśnił Wójt, było realizowanie prac naprawczych i zaleceń z poprzedniego audytu. W jednostkach podległych audyty wewnętrzne w zakresie bezpieczeństwa informacji nie były przeprowadzane w całym okresie objętym kontrolą (lata 2018-2022). W bibliotece świadomie odstąpiono od tej czynności z uwagi na bardzo małą infrastrukturę teleinformatyczną, którą stanowił jeden komputer oraz z uwagi na ceny audytów. Dyrektor Szkole Podstawowej w Wiźnie i Rutkach nie byli w stanie podać powodów nieprzeprowadzania audytów bezpieczeństwa. Zdaniem NIK właściwie przeprowadzony audyt wewnętrzny powinien ujawnić użytkowanie adresów e-mailowych na serwerach komercyjnych bez wymaganej umowy powierzenia przetwarzania danych. (akta kontroli str. 48-49, 53, 55, 262, 313-314)

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

---

[14] 1 czerwca 2021 r.

[15] Wcześniej znany też pod nazwami Macromedia Flash Player lub Shockwave Flash. Był wirtualną maszyną na której uruchamiały się pliki oraz strumienie multimedialne.

[16] XLV Sesja w dniu 15 marca 2023 r., XLIV Sesja w dniu 31 stycznia 2023 r., XLII Sesja Rady Gminy Wizna w dniu 29 listopada 2022 r., XL Sesja Rady Gminy Wizna w dniu 29 września 2022 r., XXXVII Sesja w dniu 31 maja 2022 r.

[17] Dz. U z 2023 r. poz. 775 ze zm.

[18] Dz. U. Nr 5 poz. 46.

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

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. Nieprzeprowadzanie corocznych audytów wewnętrznych w zakresie bezpieczeństwa informacji.

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.

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