NAJWYŻSZA IZBA KONTROLI

Delegatura w Białymstoku

LBI.411.003.07.2023

Pan
Andrzej Humienny
Wójt Gminy Nowy Dwór
Urząd Gminy Nowy Dwór
ul. Plac Rynkowy 21,16-205 Nowy Dwór

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 Nowy Dwór, ul. Plac Rynkowy 21, 16-205 Nowy Dwór[1]
Kierownik jednostki kontrolowanej	Andrzej Humienny, Wójt Gminy Nowy Dwór[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/51/2023 z 28 lutego 2023 r. (akta kontroli str. 1-2)

[1] Dalej: Urząd.
[2] Od 9 grudnia 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 (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]. Urząd odstąpił od obowiązku transmisji i publikacji obrad sesji organu uchwałodawczego.

Jednak już w trakcie kontroli NIK – od marca 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 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. W okresie objętym kontrolą Urząd korzystał z poczty elektronicznej pod adresem ugnowydwor@gmail.com oraz ugnd@poczta.onet.pl, a w marcu 2021 r. wykupiony został hosting na domenę gminanowydwor.pl przy czym nie oznaczało to zakończenia korzystania z pozostałych dwóch adresów e-mailowych – korzystano z trzech adresów jednocześnie i trzecim oficjalnym adresem do kontaktu e-mailowego z Urzędem był sekretariat@gminanowydwor.pl. Pracownicy Urzędu również korzystali ze skrzynek pocztowych w bezpłatnych serwisach internetowych, nawet po założeniu skrzynek e-mailowych we własnej domenie Gminy. Na skrzynce e-mailowej ugnowydwor@gmail.com znajdowały się wiadomości dotyczące bieżącego funkcjonowania Urzędu, w tym zawierające dane osobowe osób fizycznych (imiona, nazwiska, adresy zamieszkania, numery PESEL, seria i numer dowodu osobistego). Z właścicielami domen komercyjnych Urząd nie miał zawartych umów powierzenia przetwarzania danych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*. Z hostingodawcą domeny gminanowydwor.pl taką umowę zawarto 7 marca 2023 r. w trakcie kontroli NIK.

---

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

[5] W Gminnym Ośrodku Pomocy Społecznej w Nowym Dworze, Nowodworskim Ośrodku Kultury, Urzędzie Stanu Cywilnego, Szkole Podstawowej w Nowym Dworze.

[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*.

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..

Urząd Stanu Cywilnego (dalej: USC) w okresie objętym kontrolą korzystał ze skrzynki pocztowej uscnowydwor@gmail.com, a od marca 2021 r. miał założoną skrzynkę usc@gminanowydwor.pl przy czym nie była używana. Na skrzynce e-mailowej uscnowydwor@gmail.com znajdowała się korespondencja związana z załatwianiem spraw bieżących dotyczących funkcjonowania USC. Korespondencja była prowadzona wewnątrz Gminy Nowy Dwór oraz z innymi instytucjami publicznymi (w tym. Ministerstwem Spraw Wewnętrznych i Administracji, Głównym Urzędem Statystycznym, Podlaskim Urzędem Wojewódzkim) i osobami fizycznymi. Wysyłane i odbierane były wiadomości zawierające dane osobowe osób fizycznych, dane o ich stanie zdrowia (imiona, nazwiska, adresy, numery PESEL, serie i numery dowodów osobistych). Do czasu rozpoczęcia kontroli NIK, z właścicielem domeny nie zawarto umowy powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*.

Gminny Ośrodek Pomocy Społecznej w okresie objętym kontrolą korzystał ze skrzynki e-mailowej pod adresem gopsnd@poczta.onet.pl założonej na osobę fizyczną, a od marca 2021 r. miał założoną skrzynkę gops@gminanowydwor.pl przy czym nie była używana. Na skrzynce e-mailowej gopsnd@poczta.onet.pl 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 Nowy Dwór 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 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 Nowym Dworze w okresie objętym kontrolą korzystała z bezpłatnej skrzynki e-mailowej zsnd@op.pl, założonej w 2014 r. na osobę fizyczną. 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 Nowy Dwór jak też z innymi instytucjami publicznymi (m.in. Główny Urząd Statystyczny, Ministerstwo Edukacji, Kuratorium Oświaty). 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 zawarto umowy powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*. Podobnie jak pozostał jednostki podległe, Szkoła miała założoną w marcu 2021 r. skrzynkę e-mailową szkola@gminanowydwor.pl, ale nie była ona używana.

Nowodworski Ośrodek Kultury korzystał ze skrzynki e-mailowej n.d.kultura@interia.pl założonej na dane osoby fizycznej w 2012 r. Na skrzynce e-mailowej znajdowała się korespondencja związana z załatwianiem bieżących spraw, w tym m.in. faktury zakupowe oferty handlowe, korespondencja wewnątrz Gminy Nowy Dwór. Znajdowała się również korespondencja zawierająca dane osobowe, w tym m.in. imiona, nazwiska, adresy e-mail, numery telefonów, numery PESEL, wyniki badań lekarskich. Z właścicielem domeny nie była zawarta umowa powierzenia przetwarzania danych osobowych, co stanowiło naruszenie w art. 28 ust. 3 *RODO*, a ośrodek od marca 2021 r. miał założoną skrzynkę e-mailową nok@gminanowydwor.pl, ale nie była ona używana.

Przyczyną, wskazaną przez Wójta, użytkowania skrzynek e-mailowch zarówno na publicznych domenach jak też własnej domenie, bez zawartej mowy powierzenia przetwarzania danych, było przeoczenie i zaniedbanie. Po zakupie własnej domeny w marcu 2021 r. z tego też powodu niewyegzekwowano na pracownikach Urzędu i podległych jednostek zaprzestania korzystania z pozostałych adresów e-mailowych. Dla efektywnej ochrony danych osobowych Wójt widzi bariery kadrowe, finansowe praz barierę nieświadomości zagrożeń jakie wynikać mogą z zaniechań. (akta kontroli str. 3-34, 45-48, 199)

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*[8] 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*[9] i do części I.2.3 – I.2.6 *Standardów kontroli zarządczej dla sektora finansów publicznych*[10] – aby umowy takie zawarte zostały przez wszystkie gminne jednostki organizacyjne.

NIK zwraca też uwagę, że trzy z czterech jednostek organizacyjnych Gminy Nowy Dwór 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 polecono korzystać z adresów e-mailowych w domenie @gminanowydwor.pl a na 1 lipca 2023 r. zaplanowano usunięcie poprzednio używanych skrzynek w domenach komercyjnych. Przeprowadzono szkolenie pracownikom w celu zwiększenia świadomości występującego ryzyka, zobowiązano ich również do korzystania wyłącznie z poczty służbowej, a wysyłane wiadomości zawierające dane osobowe, mają być szyfrowane. (akta kontroli str. 202-203)

2. Urząd prowadził Biuletyn Informacji Publicznej na stronie internetowej https://bip-ugnowydwor.wrotapodlasia.pl/ a z właścicielem tego serwisu (Województwem Podlaskim) miał zawartą umowę powierzenia przetwarzania danych osobowych[11]. W BIP publikowane były m.in. oświadczenia majątkowe osób, o których mowa w art. 24h ust. 1 ustawy o samorządzie gminnym, przy czym 418 (z 599, tj. 70%) przechowywano ponad sześć lat, najstarsze złożone były za 2013 r. 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 był brak dostatecznego nadzoru nad tym procesem oraz brak komunikacji między pracownikiem Urzędu a współpracownikiem zatrudnionym na podstawie umowy cywilno-prawnej, obsługującym stronę BIP.

---

[8] Dz. U. z 2019 r. poz. 1781. Dalej: *uodo*.
[9] Dz. U. z 2022 r. poz. 1634, ze zm.
[10] Ogłoszonych Komunikatem Nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. (Dz. Urz. MF Nr 15, poz. 84).
[11] 7 maja 2021 r.

Oświadczenia majątkowe które były opublikowane w BIP w dniu rozpoczęcia kontroli[12], a dla których minął okres retencji danych, zostały z BIP usunięte 5 marca 2023 r.

(akta kontroli str. 35-39)

3. Urząd nie wywiązywał się z publikacji odbywających się sesji organów uchwałodawczych – o czym mowa w art. 20 ust. 1b *ustawy o samorządzie gminnym*. W okresie objętym kontrolą żadna transmisja z obrad sesji Rady Gminy nie została opublikowana. Publikacji podlegały jedynie protokoły z poszczególnych obrad[13]. W trakcie kontroli podjęto działania, aby realizować ustawowy obowiązek w tym zakresie, wykonano rozeznanie rynku i podjęto działania w celu wyłonienia usługodawcy w tym zakresie. Wójt wyjaśnił, że przyczyną braku transmisji były kwestie finansowe, niemniej wykonano rozeznanie kosztów ewentualnej usługi wśród firm, które na rynku lokalnym świadczą takie usługi i podjęto zostaną kroki mające na celu wyłonienia dostawcy usług w zakresie obsługi transmisji obrad sesji Rady Gminy.

(akta kontroli str. 36-39, 201, 205)

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. Nie stwierdzono jednak takich publikacji na BIP. (akta kontroli str. 204)

5. Zarówno w Urzędzie jak też podległych jednostkach w latach 2018-2021 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*[14]. W 2022 r. w Urzędzie przeprowadzony został audyt wewnętrzny w zakresie ochrony danych osobowych, w którym stwierdzono, że administrator dołożył wszelkich starań, by poziom ochrony danych osobowych był jak najwyższy. Najwyższa Izba Kontroli zauważa, że audyt ten nie stwierdził braku umów powierzenia przetwarzania danych z hostingodawcą i operatorami serwisów internetowych z darmową pocztą elektroniczną. Wójt wyjaśnił, że powodem nieprzeprowadzania audytów w pozostałych latach było zaniedbanie oraz względy finansowe i kadrowe. (akta kontroli str. 46-47, 58-80)

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 418 oświadczeń majątkowych, dla których minął sześcioletni okres przechowywania (retencji danych).
3. Niewywiązanie się z obowiązku publikacji transmisji z obrad organu uchwałodawczego Gminy Nowy Dwór.
4. Nieprzeprowadzanie corocznych audytów wewnętrznych w zakresie bezpieczeństwa informacji.

Zdaniem NIK działania naprawcze wdrożone przez Urząd w okresie od marca do maja 2023 roku wskazane w punktach 1-3 *Opisu ustalonego staniu faktycznego* doprowadziły do usunięcia nieprawidłowości stwierdzonych w p-ktach 1-3 lub zaplanowano ich usunięcie.

---

[12] 1 marca 2023 r.

[13] https://bip-ugnowydwor.wrotapodlasia.pl/-u--b-organy-gminy--b---u-/rada-gminy/sesje-rady/

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

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. Spełnienie obowiązku publikacji odbywających się sesji Rady Gminy.
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.

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