NAJWYŻSZA IZBA KONTROLI
Delegatura w Białymstoku

LBI.411.003.08.2023

Pan
Lech Marek Szabłowski
Starosta Łomżyński
Starostwo Powiatowe w Łomży
ul. Szosa Zambrowska 1/27, 18-400 Łomża

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	Starostwo Powiatowe w Łomży, ul. Szosa Zambrowska 1/27, 18-400 Łomża[1]
Kierownik jednostki kontrolowanej	Lech Marek Szabłowski, Starosta Łomżyński[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/68/2023 z 24 marca 2023 r. (akta kontroli str. 1-2)

[1] Dalej: Starostwo.
[2] Od 21 listopada 2018 r., wcześniej tą funkcję w okresie objętym kontrolą pełniła Elżbieta Parzych.
[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 Starosta 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 Starostwo w formie elektronicznej oraz nie realizował skutecznej i adekwatnej kontroli zarządczej w tym zakresie na poziomie jednostki samorządu terytorialnego (powiatu).

W czterech[5] powiatowych 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 Starostwie 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. 25c ust. 6 *ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym*[7]. Transmitowanie i upublicznianie przez Starostwo sesji organu uchwałodawczego odbywało się bez przeprowadzenia wymaganej analizy ryzyka, wynikającej z korzystania z jednego z serwisów internetowych, podczas przetwarzania danych osobowych uczestników sesji Rady Powiatu.

Jednak już w trakcie kontroli NIK – od marca do maja 2023 r. – Starostwo podjęło 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 Powiatu zostało usuniętych zarówno w Starostwie, jak i jednostkach organizacyjnych powiatu, 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. Starostwo korzystało z poczty elektronicznej pod adresem starostwo@powiatlomzynski.pl którą utworzyło w 2017 roku (wcześniej również z adresu starostwo.blm@powiatypolskie.pl). Pracownicy Urzędu korzystali z imiennych skrzynek e-mailowych w tej samej domenie @powiatlomzynski.pl. Z hostingodawcą zawarta była umowa powierzenia przetwarzania danych, na podstawie art. 28 ust. 3 *RODO*[8].

W latach 2018-2022 Starosta nie prowadził skutecznej i adekwatnej kontroli zarządczej w powiatowych jednostkach organizacyjnych w zakresie bezpieczeństwa danych, w tym danych osobowych gromadzonych przez te jednostki w formie elektronicznej.

Zakład Podstawowej Opieki Zdrowotnej w Łomży korzystał ze skrzynki e-mailowej pod adresem zpozstat@wp.pl i sekretariatzpoz@wp.pl, były to skrzynki bezpłatne założone na osobę fizyczną. Pracownicy Zakładu korzystali ze skrzynek e-mailowych w serwisach wp.pl, onet.pl i gmail.com. Na skrzynkach e-mailowych znajdowała się korespondencja związana

---

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

[5] W Poradni Psychologiczno-Pedagogicznej, Powiatowym Centrum Pomocy Rodzinie, Muzeum w Drozdowie i Zakładzie Podstawowej Opieki Zdrowotnej.

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

[7] Dz. U. z 2022 r. poz. 1526, ze zm. Ustawa zwana dalej *ustawą o samorządzie powiatowym.*

[8] 25 czerwca 2021 r.

z załatwianiem spraw bieżących dotyczących funkcjonowania Zakładu, w szczególności z dostawcami produktów leczniczych, rozliczaniem świadczeń opieki zdrowotnej z Podlaskim Oddziałem Wojewódzkim Narodowego Funduszu Zdrowia oraz w związku z kontrolami tego podmiotu, w sprawach osobowych. Wysyłane i odbierane były wiadomości zawierające dane osobowe osób fizycznych, (imiona, nazwiska, adresy, numery PESEL, telefon kontaktowy, korzystanie z określonych preparatów medycznych). 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*.

Powiatowe Centrum Pomocy Rodzinie korzystało ze skrzynki e-mailowej pod adresem pcprlomza@wp.pl, była to skrzynka bezpłatna założona na osobę fizyczną. Na skrzynce e-mailowej znajdowała się korespondencja związana z załatwianiem spraw bieżących dotyczących funkcjonowania Centrum i realizacją zadań własnych powiatu z zakresu wspierania rodziny i systemu pieczy zastępczej, w szczególności z innymi centrami pomocy i jednostkami organizacyjnymi w ramach Powiatu Łomżyńskiego i poza nim. Wysyłane i odbierane były wiadomości zawierające dane osobowe osób fizycznych, (imiona, nazwiska, adresy, numery PESEL, seria i numer dowodu osobistego, telefon kontaktowy, opis sytuacji rodzinnej i zdrowotnej). 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*.

Poradnia Psychologiczno-Pedagogiczna korzystała ze skrzynki e-mailowej pod adresem poradniapp1lomza@poczta.fm, była to skrzynka bezpłatna założona na osobę fizyczną. Na skrzynce e-mailowej znajdowała się korespondencja związana z załatwianiem spraw bieżących dotyczących funkcjonowania Poradni i z realizacji zadań własnych powiatu z zakresu edukacji publicznej, w szczególności z Podlaskim Kuratorem Oświaty, placówkami oświatowymi i jednostkami organizacyjnymi w ramach Powiatu Łomżyńskiego i poza nim. Wysyłane i odbierane były wiadomości zawierające dane osobowe osób fizycznych, (imiona, nazwiska, adresy, numery PESEL, telefon kontaktowy, opis diagnozy). 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*. (akta kontroli str. 5-35)

Najwyższa Izba Kontroli zauważa, że zarówno w Poradni Psychologiczno-Pedagogicznej jak też Powiatowym Centrum Pomocy Rodzinie były prowadzone coroczne audyty wewnętrzne z zakresu bezpieczeństwa informacji, o których mowa w § 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*[9], które powinny ujawnić brak umów powierzenia przetwarzania danych z komercyjnym dostawcą usługi poczty elektronicznej, jednak nie zidentyfikowały takiego ryzyka. Z kolei w Zakładzie Podstawowej Opieki Zdrowotnej i Muzeum w Drozdowie nie przeprowadzano takich audytów w okresie objętym kontrolą. Powodem nieprzeprowadzania takich audytów były m.in. bariery finansowe, bariery nieświadomości, w tym nieświadomości zagrożeń.

Jak wyjaśnili kierownicy poszczególnych jednostek organizacyjnych powiatu, przyczynami korzystania ze skrzynek e-mailowych na portalach komercyjnych, bez zawartej umowy powierzenia przetwarzania danych z procesorem[10], był przede wszystkim brak świadomości kierownictwa tych jednostek o potrzebie zawarcia takiej umowy, przekonanie o bezpieczeństwie przetwarzanych danych, zaszłości historyczne – kontynuowanie pracy z użyciem tej skrzynki pocztowej po zmianie kierownictwa jednostki.

(akta kontroli str. 63-66, 77-80, 88-89, 93-96)

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 jednostki organizacyjne powiatu jako podmioty sektora finansów publicznych są samodzielnymi administratorami danych. Dla zabezpieczenia danych osobowych, przetwarzanych w powiecie, jako jednostce samorządu terytorialnego, w związku z wykonywaniem zadań publicznych jej przypisanych wskazane jest wdrożenie

---

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

[10] Podmiot który przetwarzanie dane osobowe.

[11] Dz. U. z 2019 r. poz. 1781. Ustawa zwana dalej: *uodo*.

odpowiednich środków technicznych i organizacyjnych, zapewniających bezpieczeństwo przetwarzania tych danych zarówno w Starostwie, jak i we wszystkich jednostkach organizacyjnych powiatu. 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*.

Starosta – będący zgodnie z art. 35 ust. 2 *ustawy o samorządzie powiatowym* kierownikiem Starostwa i zwierzchnikiem służbowym kierowników jednostek organizacyjnych powiatu – powinien zawrzeć taką umowę, dotyczącą Starostwa 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 powiatowe jednostki organizacyjne.

NIK zwraca też uwagę, że dwie z siedmiu jednostek organizacyjnych Powiatu Łomżyńskiego funkcjonują w ramach osobowości prawnej tego Powiatu, 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 byłby powiat 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 wszystkie jednostki zaprzestały korzystać ze skrzynek e-mailowych w domenach komercyjnych. Powiatowe Centrum Pomocy Rodzinie oraz Poradnia Psychologiczno-Pedagogiczna uzyskały możliwość korzystania z poczty e-mailowej w domenie @powiatlomznski.pl, Zakład Podstawowej Opieki Zdrowotnej założył pocztę na wykupionej domenie zpozlomza.pl, a Muzeum w Drozdowie w domenie muzeum-drozdowo.pl.

(akta kontroli str. 67, 81, 97, 162)

2. Starostwo prowadziło Biuletyn Informacji Publicznej na stronie internetowej https://powiatlomzynski.pl/bip/ a z hostingodawcą miało zawartą umowę powierzenia przetwarzania danych osobowych[14]. W BIP publikowane były m.in. oświadczenia majątkowe osób, o których mowa w art. 25c ust. 1 *ustawy o samorządzie powiatowym*, przy czym 89 (z 467, tj. 19%) przechowywano ponad sześć lat, najstarsze złożone były za 2010 r. Było to niezgodne zarówno z art. 25c ust. 6 *ustawy o samorządzie powiatowym* 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*. Starosta wyjaśnił, że powodem publikacji oświadczeń po terminie retencji danych było rozproszenie tych danych w różnych folderach. Poprzez co zostało pominięte.

Oświadczenia majątkowe które były opublikowane w BIP w dniu rozpoczęcia kontroli[15], a dla których minął okres retencji danych, zostały z BIP usunięte 14 kwietnia 2023 r.

(akta kontroli str. 4, 39)

3. Do realizowania obowiązku publikacji odbywających się sesji organów uchwałodawczych – o czym mowa w art. 15 ust. 1a *ustawy o samorządzie powiatowym* – Starostwo wykorzystywało portal *YouTube*, na którym opublikowano 37 sesji Rady Powiatu. 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

---

[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).

[14] 31 grudnia 2021 r.

[15] 24 lutego 2023 r.

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*. Starosta stał na stanowisku, że kategorie osób których dane dotyczą, zawężone są tylko do osób wypełniających funkcje publiczne. Przewodniczący Rady po rozpoczęciu posiedzenia Rady informuje zebranych o transmisji i utrwalaniu obrad za pomocą urządzeń rejestrujących dźwięk i obraz, zaś w sytuacji gdyby w części powiedzenia inna osoba chciałaby zabrać głos – przewidziane jest uzyskanie pisemnego oświadczenia wyrażenia zgody tej osoby na upublicznienie wizerunku. Najwyższa Izba Kontroli zauważa jednak, że w przypadku bezpłatnego konta na portalu *YouTube* – a z takiego korzystało Starostwo – nie jest możliwe zawarcie umowy powierzenia przetwarzania danych osobowych w postaci wizerunku, nie jest również możliwe wskazanie miejsca przechowywania danych, aby nie było to poza obszarem Europejskiego Obszaru Gospodarczego (EOG) i w efekcie miejsce przechowywania danych przez portal jest nieznane. Sam fakt uzyskania oświadczenia o wyrażeniu zgody na publikację wizerunku, niezależnie od tego, czy ta osoba pełni funkcję publiczną czy też nie, nie stanowi przesłanki legalizującej przekazywanie go do krajów poza EOG. Zgoda taka nie stanowi zatem przesłanki do przekazywania danych osobowych do kraju trzeciego, stanowiącej wyjątek w szczególnych sytuacjach, o których mowa w 49 ust. 1 *RODO*.

Na próbie pięciu[16] (z 20 sesji) ustalono, że wywiązano się z obowiązku transkrypcji obrad, nałożonego 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*[17] (napisy rozszerzone i audiodeskrypcja). (akta kontroli str. 36-41, 122-124, 213-214)

Starosta wyjaśnił również, że w ramach realizowanych projektów zostanie zakupiony i wdrożony system obsługi rady powiatu, zapewniający platformę streamingową (na serwerach dostawcy usługi znajdujących się w Polsce) dla relacji z obrad Rady Powiatu Łomżyńskiego. (akta kontroli str. 124)

4. W kontrolowanym okresie wpłynęły do Starostwa trzy skargi na Starostę i/lub kierowników jednostek mu podległych, rozpatrzone przez Radę Powiatu[18]. Opublikowane uchwały były właściwie zanonimizowane i dane skarżących nie zostały ujawnione. (akta kontroli str. 215)

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 jednostki organizacyjne powiatu.
2. Publikowanie w BIP 89 oświadczeń majątkowych, dla których minął sześcioletni okres przechowywania (retencji danych).
3. Powierzenie przetwarzania danych osobowych osób uczestniczących w 37 sesjach Rady Powiatu właścicielowi serwisu *YouTube* bez przeprowadzenia odpowiedniej analizy ryzyk i bez zawarcia umowy powierzenia przetwarzania danych osobowych.

Zdaniem NIK działania naprawcze wdrożone przez Starostwo 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, 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 Powiatu z serwisu *YouTube* lub zawarcie umowy powierzenia przetwarzania danych z właścicielem tego serwisu.

---

[16] Transmisje: XXXVII, XXXVI, XXXII, XXVII, XXIII sesji Rady Powiatu Łomżyńskiego.

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

[18] W uchwałach Nr XXXIII/175/2018 z 7 marca 2018 r., Nr IX/55/2019 z 4 września 2019 r. i Nr XXXI/200/2022 z 14 września 2022 r.

2. Kontynuowanie działań w zakresie kontroli zarządczej na poziomie powiatu, w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych, gromadzonych w formie elektronicznej, zarówno przez Starostwo jak i jednostki organizacyjne powiatu.

Z uwagi na działania podjęte w Starostwie, 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