NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.410.017.06.2021

Marzanna Wardziejewska
Starosta Powiatu Gołdapskiego
ul. Krótka 1
19-500 Gołdap

WYSTĄPIENIE POKONTROLNE

P/21/081 – Bezpieczeństwo informacji w pracy na odległość i mobilnym przetwarzaniu danych

NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie
ul. Artyleryjska 3e, 10-165 Olsztyn
T +48 89 678 82 00, F +48 89 678 82 30
lol@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana: Starostwo Powiatowe w Gołdapi, ul. Krótka 1, 19-500 Gołdap (dalej: „Starostwo").

Kierownik jednostki kontrolowanej: Marzanna Wardziejewska, Starosta Powiatu Gołdapskiego od 23 listopada 2018 r. („Starosta").

Zakres przedmiotowy kontroli:

1. Organizacja bezpieczeństwa pracy.
2. Wdrożone i stosowane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji w pracy zdalnej.

Okres objęty kontrolą: Lata 2020-2021 (do dnia zakończenia kontroli[1]), z uwzględnieniem zdarzeń wcześniejszych, jeżeli miały one wpływ na kontrolowane obszary działalności.

Podstawa prawna podjęcia kontroli: Art. 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2].

Jednostka przeprowadzająca kontrolę: Najwyższa Izba Kontroli Delegatura w Olsztynie.

Kontroler: Edward Odojewski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/124/2021 z 11 października 2021 r.

(akta kontroli str.1-3)

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA: Najwyższa Izba Kontroli pozytywnie ocenia realizację przez Starostwo, w okresie objętym kontrolą, zadań w zakresie bezpieczeństwa informacji w pracy na odległość i mobilnym przetwarzaniu danych.

Uzasadnienie oceny ogólnej: Starostwo zapewniło warunki organizacyjne do realizacji zadań objętych kontrolą. Opracowano oraz wdrożono w tym celu odpowiednie zasady systemu zarządzania bezpieczeństwem informacji, obejmujące politykę tego bezpieczeństwa i instrukcję zarządzania systemem informatycznym w Starostwie, z uwzględnieniem przepisów krajowych i UE w zakresie ochrony danych osobowych, w tym krajowych ram interoperacyjności i polskich norm. Zasady te poddawano regularnym przeglądom, wyciągając z nich wnioski organizacyjne. Powołano też inspektora ochrony danych osobowych, który posiadał odpowiednie przygotowanie zawodowe i kwalifikacje oraz brał udział w szkoleniach specjalistycznych. Przydzielono mu obowiązki wynikające z tych przepisów, za wyjątkiem audytowania zagadnień związanych z ochroną danych osobowych, gdyż zadanie to było obowiązkiem audytora wewnętrznego. Odpowiedzialność za bezpieczeństwo teleinformatyczne oraz administrowanie zasobami informacji ponosił informatyk urzędu, prowadząc odpowiednie rejestry posiadanego sprzętu/aktywów informatycznych. Wprowadzone zasady i rozwiązania techniczno-technologiczne, które uwzględniały zidentyfikowane ryzyka, zapewniły odpowiedni poziom bezpieczeństwa informacji oraz jakość i ciągłość funkcjonowania urzędu w warunkach epidemii COVID-19, przy czym ich aktualizacja podniosła ten poziom adekwatnie do zagrożenia epidemią. Wdrażając te regulacje zorganizowano odpowiednie szkolenie wewnętrzne dla wszystkich pracowników oraz zapoznawano ich z aktualizacją lub modyfikacją zasad dotyczących bezpieczeństwa informacji, w tym warunków pracy zdalnej i rotacyjnej.

---

[1] 29 listopada 2021 r.

[2] Dz. U. z 2020 r. poz. 1200, ze zm. (dalej: „ustawa o NIK").

[3] NIK formułuje ocenę ogólną, jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

III. Opis ustalonego stanu faktycznego i oceny cząstkowe[4] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1. Zgodnie z § 20 ust. 1 rozporządzenia ws. krajowych ram interoperacyjności[5], w Starostwie opracowano i wprowadzono do stosowania[6] Politykę Bezpieczeństwa Informacji („PBI") oraz Instrukcję Zarządzania Systemem Informatycznym („IZSI"), które w myśl tego rozporządzenia stanowiły System Zarządzania Bezpieczeństwem Informacji („SZBI"). System ten opracowano wg Polskiej Normy PN-ISO/IEC 27001 (§ 20 ust. 3 KRI), a ustanowienie zabezpieczeń, zarządzanie ryzykiem i audyt odbywały się na podstawie Norm[7] związanych z ww. PN. Do przestrzegania tych regulacji zostali zobowiązani wszyscy pracownicy Starostwa, którzy zapoznali się z ich treścią, co potwierdzili podpisując stosowne oświadczenie (wg załączonej do zarządzenia listy). Do akt personalnych każdego z nich (44 osoby) załączono zaś oświadczenie, w którym potwierdzili oni zapoznanie się z przepisami rozporządzenia ws. ochrony osób fizycznych w zw. z przetwarzaniem danych osobowych[8] oraz zobowiązali się do ich stosowania, w tym regulacji wewnętrznych obowiązujących w tym zakresie oraz zachowania w tajemnicy danych osobowych, także po ustaniu zatrudnienia. Oświadczenia takie wyegzekwowano także od 24 osób, które zatrudniano w terminie późniejszym, tj. po 24 maja 2018 r. Mimo, że powyższe oświadczenie należało jako oświadczenie o poufności złożyć wg wzoru określonego w załączniku nr 1 do PBI, w przypadku 56 osób (49 w 2018 r. i siedmiu w 2019 r.) nie dopełniono jednak tego wymogu i przyjęto oświadczenia wg innej formy, której konstrukcja nie odpowiadała treści określonej ww. załącznikiem i nie zawierała przewidzianych w nim zobowiązań, gdyż nie wymagała zabezpieczenia danych osobowych po odwołaniu upoważnienia lub zakończeniu współpracy i nie odnosiła się wprost do regulacji SZBI, lecz tylko ogólnie do bliżej nieokreślonych regulacji w zakresie przetwarzania danych.

Inspektor Ochrony Danych („IOD") wyjaśniła, że zmieniona forma ww. oświadczenia wynikała z wiedzy powziętej podczas szkoleń wz. zarządzania bezpieczeństwem informacji, lecz przez przeoczenie nie dokonano aktualizacji wzoru tego załącznika. Od 2020 r. powrócono jednak do przyjmowania oświadczeń w formie przewidzianej wg zał. Nr 1 do PBI, która spełniała wymogi bezpieczeństwa przetwarzania danych.

W urzędzie zidentyfikowano informacje, pozostałe aktywa z nimi związane oraz środki wykorzystywane do ich przetwarzania, jak też sporządzono i utrzymywano aktualność ewidencji tych aktywów. Wdrożony SZBI był adekwatny do potencjalnych zagrożeń jakie mogły wystąpić, tj. określał zasady, aktywa i środki wykorzystywane do przetwarzania danych. Zasady te dotyczyły m.in. postępowania z nośnikami, zarządzania uprawnieniami użytkowników, bezpieczeństwa aktywów wynoszonych poza Starostwo i pozostawiania ich bez opieki, zabezpieczenia sieci, w tym przed

---

[4] Oceny cząstkowe to oceny działalności w poszczególnych obszarach kontrolnych. Ocena cząstkowa może być sformułowana, jako ocena pozytywna, negatywna albo w formie opisowej.

[5] Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. ws. Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych – dalej: „KRI" (Dz. U. z 2017 r. poz. 2247).

[6] Zarządzenie Nr 33/2018 Starosty z 24 maja 2018 r. ws. wprowadzenia Polityki bezpieczeństwa przetwarzania danych osobowych oraz Instrukcji zarządzania systemem informatycznym w Starostwie.

[7] PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – do zarządzania ryzykiem, PN-ISO/IEC 24762 – do odtwarzania techniki informatycznej po katastrofie.

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. ws. ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i ws. swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – dalej: „RODO" (Dz. Urz. UE z 2016 r. poz. 119).

szkodliwym oprogramowaniem, przesyłania danych w formie elektronicznej i ich zabezpieczenia oraz zarządzania incydentami.

(akta kontroli str. 4-210, 255-269, 307-308)

1.2. Zgodnie z wymogami Polskiej Normy PN-ISO/IEC 27001, Starosta w ramach SZBI określił obowiązki, uprawnienia i zakres odpowiedzialności pracowników za bezpieczeństwo informacji, przydzielając te kompetencje osobom pełniącym istotną rolę w jego zapewnieniu. Zadania w tym zakresie obejmowały przede wszystkim analizę ryzyka i incydentów oraz aktualizację obowiązujących zasad i procedur, za co odpowiadał IOD. Za bezpieczeństwo informacji odpowiadali wszyscy pracownicy Starostwa, którzy wg przydzielonego im zakresu odpowiedzialności mieli obowiązek zabezpieczenia przyjętego do używania sprzętu, właściwego kompletowania, przechowywania, gromadzenia i zabezpieczenia dokumentacji i baz danych oraz ochrony danych przed dostępem osób nieuprawnionych, nieuzasadnioną modyfikacją, zniszczeniem, nielegalnym ujawnieniem/pozyskaniem. Informatyczną obsługę Starostwa zapewniał informatyk urzędu jako administrator systemów informatycznych (dalej: „ASI"), który wdrażał politykę bezpieczeństwa i zarządzania aktywami, koordynował projekty związane z informatyzacją, instalował programy komputerowe i udzielał instrukcji, prowadził ewidencję sprzętu komputerowego i oprogramowania oraz zapewniał ich przeglądy i konserwację, a także monitorował legalność ich używania przez pracowników oraz nadzorował prawidłowość działania infrastruktury teleinformatycznej w urzędzie.

(akta kontroli str. 211, 236-238, 243)

1.3.1. W myśl art. 37 ust. 1 RODO oraz zgodnie z Regulaminem Organizacyjnym[9], Starosta powołała[10] IOD, przydzielając mu zadania z art. 39 RODO, w tym m.in.:

- informowanie ASI, personelu Starostwa i jednostek organizacyjnych Powiatu, którzy przetwarzają dane osobowe, o ich obowiązkach na mocy przepisów o ochronie danych i doradzanie im w tej sprawie,
- monitorowanie przestrzegania przepisów krajowych i UE oraz polityk administratora lub podmiotu przetwarzającego o ochronie danych, w tym podział obowiązków, zwiększanie świadomości personelu przetwarzającego dane i jego szkolenia; w ramach tych zadań brakowało zapisu odnoszącego się do obowiązku prowadzenia powiązanych z nimi audytów, co wg Starosty wynikało z przeoczenia, a w PBI zadanie to zostało uwzględnione;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO,
- współpracę z organem nadzorczym i pełnienie funkcji punktu kontaktowego w zakresie przetwarzania, w tym z uprzednimi konsultacjami (art. 36 RODO) oraz ich prowadzenie we wszelkich innych sprawach.

IOD był ponadto zobowiązany do prowadzenia dokumentacji związanej z ochroną danych osobowych, w tym rejestru czynności i incydentów oraz sprawozdań w tym zakresie, a także dokonywania oceny i szacowania ryzyka celem zastosowania skutecznych metod organizacyjno-technicznych dla właściwej ochrony danych lub oceny skutków jej naruszenia. Zadania IOD ujęto w szczegółowym podziale zadań pomiędzy komórki organizacyjne i samodzielne stanowiska w Starostwie[11].

(akta kontroli str. 212-235, 239-248, 309-314)

Ze sprawozdania audytora wewnętrznego, który w okresie od 18 lutego do 20 marca 2020 r. przeprowadził zadanie audytowe względem stanowiska IOD, wynikało, że wśród jego obowiązków nie było obowiązku dotyczącego prowadzenia audytów

[9] Uchwała Zarządu Powiatu Nr 135/2017 z 25 maja 2017 r. ws. Regulaminu Organizacyjnego Starostwa, zm. uchwałą Nr 201/2018 z 16 maja 2018 r.

[10] Zarządzenie Starosty Nr 31/2018 ws. powołania inspektora ochrony danych (ze zm. 5 października 2021 r.).

[11] Zarządzenie Starosty Nr 50/2018 z 27 września 2018 r., zm. zarządzenie Nr 22/2017 z 5 czerwca 2017 r.

w zakresie ochrony danych osobowych. Badania audytora objęły wykonywanie obowiązków IOD w świetle przepisów prawa powszechnego i wewnętrznego, w tym rozporządzenia RODO. W wyniku badań audytor nie stwierdził uchybień oraz nie sformułował żadnych zaleceń, wskazując na pozytywną oceną funkcjonowania IOD.

(akta kontroli str. 376-387)

1.3.2. Zgodnie z wymogami art. 37 ust. 5 RODO, IOD był należycie przygotowany do pełnienia tej funkcji poprzez odpowiednie kwalifikacje i umiejętności zawodowe, w tym wyższe wykształcenie w kierunku zarządzania (organizacja i administrowanie) oraz wiedzę fachową nabytą w wyniku udziału w szkoleniach specjalistycznych[12], dotyczących: ochrony danych, zadań IOD i administratorów, szacowania ryzyka i oceny skutków dla przetwarzania danych, prawa i praktyk w zakresie ochrony danych i umiejętności wypełniania zadań oraz krajowych ram interoperacyjności, co potwierdziły uzyskane certyfikaty wydane przez uprawnione firmy szkolące[13].

(akta kontroli str. 249, 315)

1.4. Zgodnie z PN-ISO/IEC 27001 (zał. A pkt 8.3), zasady bezpieczeństwa ujęte w IZSI uwzględniały czynności i ryzyka w celu zapobiegania nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu danych, w tym na nośnikach elektronicznych i VPN. Postępowanie z nośnikami wymagało, aby ich użytkownicy:

- nie pozostawiali bez opieki w miejscach publicznych nośników wymiennych przetwarzających informacje administratora danych,
- przewozili komputery przenośne jako bagaż podręczny i w miarę możliwości je maskowali,
- dbali o należyte zabezpieczenie powierzonego sprzętu i baz danych przed dostępem osób trzecich oraz nie udostępniali im tych aktywów,
- zgłaszali bezpośredniemu przełożonemu, IOD/ASI przypadki utraty sprzętu komputerowego i problemy dotyczące jego nieprawidłowego działania.

Powyższe zasady zarządzania nośnikami były zgodne z przyjętym w Starostwie schematem klasyfikacji informacji. Prowadzono również aktualną ewidencję[14] nośników służących do przechowywania informacji, przypisując pracownikom odpowiedzialność za dany nośnik. W zależności od klasy informacji, zasady bezpieczeństwa zapewniały ich poufność i ochronę fizyczną oraz uwzględniały wykorzystanie kluczy kryptograficznych w przypadku transmisji wrażliwych danych osobowych i informacji wewnętrznych jednostki. Za generowanie tych kluczy, ich przechowywanie i bezpieczną dystrybucję odpowiadał ASI. W przypadku ich niestosowania, ww. dane należało przesyłać wyłącznie pocztą elektroniczną po aktywacji funkcji podpisywania i szyfrowania plików. Wdrożone zasady nie zakładały korzystania z pamięci przenośnych (pendrive, płyty CD/DVD) do kopiowania lub transportu informacji zapisanych w plikach komputerowych, jak też ochrony informacji zawartych w tradycyjnych dokumentach papierowych lub wydrukach komputerowych jako nośnikach informacji.

(akta kontroli str. 47-101, 196, 199-200, 253-254, 259, 271-295, 316-323)

1.5. Zgodnie z § 20 ust. 2 pkt 11 KRI, Pracodawca określił zasady wynoszenia aktywów, w tym sprzętu oraz nośników, a także oryginałów i kopii dokumentów, celem minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania

---

[12] Szkolenia RODO: Akademia Kształcenia Kadr/Skierniewice - 9 maja 2018 r., OS „Edytor"/Łomża - 10 lipca 2018 r. i 15 grudnia 2020 r.; seminarium/szkolenie – „EKO-MAR"/Tarnobrzeg, 20-21 listopada 2019 r.; szkolenia – ISO-LEX/Jastrzębie-Zdrój – 19 listopada 2020 r. i 16 lutego 2021 r.

[13] Posiadające stosowne uprawnienia i wpisane do rejestru instytucji szkoleniowych.

[14] Ewidencję prowadzono komputerowo w programie IT MANAGER/INFONED PROJEKT SA, na podstawie licencji dla 50 stanowisk z terminem ważności do 27 grudnia 2023 r., zakupionej za kwotę 7,7 tys. zł oraz polisą za 5,4 tys. zł, w procedurze zamówień o wartości do 4 tys. euro, wg regulaminu wprowadzonego zarządzeniem Starosty Nr 19/2014 z 16 kwietnia 2014 r.

(urządzeń mobilnych). Spełniając wymogi PN-ISO/IEC 27001, wprowadził również regulacje mające zapobiegać utracie lub uszkodzeniu integralności aktywów oraz zakłóceniom w działaniu urzędu, a także podał metody zabezpieczeń prowadzących do osiągnięcia tych celów (pkt A.11.2). W związku z wynoszeniem aktywów zostały określone podstawowe ryzyka oraz mechanizmy i sposoby zabezpieczenia przed zdarzeniami wynikającymi z wystąpienia zagrożeń.

Do zasad pracy zdalnej należy zaliczyć m.in. zalecenie korzystania ze sprzętu służbowego po odpowiednim przeglądzie oraz pobranego za protokołem (komputer, laptop, smartfon, tablet) lub prywatnego za zgodą Pracodawcy, zakaz udostępniania sprzętu innym osobom, używanie legalnego oprogramowania, do którego włączono automatyczne aktualizacje, zaporę systemową i sprawny program antywirusowy oraz zastosowanie uwierzytelnienia (login, hasło, kod PIN), program szyfrujący dane (np. 7-zip) i automatyczną blokadę urządzenia przy dłuższym braku aktywności. Pracodawca mógł wymagać, aby wykorzystywany do pracy sprzęt zawierał także inne zabezpieczenia, w tym oprogramowanie służące monitorowaniu wykonywanej pracy, zgodnie z przepisami prawa pracy. W przypadku korzystania z dokumentów w formie papierowej, obowiązywał ogólny zakaz ich wynoszenia poza siedzibę, co wynikało z wdrożenia elektronicznego obiegu dokumentów i dostępu do nich za pośrednictwem poczty elektronicznej. W razie potrzeby skorzystania z dokumentów papierowych, pracownik mógł uzyskać pisemną zgodę naczelnika wydziału na ich skopiowanie i zabranie poza siedzibę Starostwa na czas pracy zdalnej, która nie mogła odbywać się w miejscach publicznych.

Osoby pracujące zdalnie obowiązywał m.in. zakaz udostępniania innym osobom haseł uwierzytelniających dostęp do systemów i usług, przekazywania tych haseł tą samą drogą komunikacji co zabezpieczone pliki, korzystania z urządzeń, które nie zostały zatwierdzone przez pracodawcę, logowania się na konto innego pracownika i niszczenia dokumentów w domu, z uwagi na obowiązek ich kompletnego zwrotu.

(akta kontroli str. 178-183)

1.6. Na potrzeby pracy zdalnej oraz zapewnienia pracownikom możliwości wymiany informacji, w Starostwie stosowano odpowiednie regulacje technologiczne, które zapewniały bezpieczne przesyłanie informacji pomiędzy wszystkimi pracownikami, jak też pomiędzy nimi, a systemami gromadzenia i przetwarzania danych. Sposoby komunikacji z pracownikami zdalnymi posiadały zabezpieczenia adekwatne do potencjalnych zagrożeń. Zabezpieczenie przekazywanych danych polegało na używaniu tylko programów, systemów oraz serwerów udostępnionych przez Pracodawcę, zabezpieczaniu hasłem[15] informacji przesyłanych elektronicznie, stosowaniu haseł odpowiednio skomplikowanych , sprawdzaniu adresów odbiorców, stosowaniu tzw. ukrytej kopii (UDW/BCC) oraz specjalnego oprogramowania do wysyłania danych do kilku odbiorców (wysyłki masowe). Należało zapewnić poufność haseł i niezwłocznie je zmieniać w razie podejrzenia lub rzeczywistego ujawnienia oraz informować o tym ASI i IOD. ASI miał obowiązek skonfigurować system w taki sposób, aby próby dostępu były limitowane w ujęciu ilościowym i czasowym – po trzech błędnych próbach logowania następowała blokada konta, z możliwością odblokowania lub zresetowania hasła przez ASI i poinformowania o tym użytkownika. Ograniczono również możliwość wielokrotnego logowania na kilku komputerach jednocześnie z wykorzystaniem tego samego loginu.

Celem zabezpieczenia przesyłanych informacji, wprowadzone zasady zezwalały też na obsługę służbowej poczty elektronicznej z komputerów własnych pracownika, pod warunkiem spełniania podstawowych wymogów bezpieczeństwa, tj. posiadania

[15] Należało stosować hasła składające się z min. 8 znaków zawierających kombinację małych i dużych liter oraz cyfr i znaków specjalnych; hasła nie mogły zawierać w swojej strukturze części login, a po zmianie (nie rzadziej niż raz na 30 dni) być zbliżone do haseł poprzednich.

legalnego oprogramowania, aktualnego systemu operacyjnego oraz programu antywirusowego, a także możliwości szyfrowania danych. Pracownicy mieli obowiązek korzystania głównie ze służbowych kont e-mail, lecz w przypadku przetwarzania danych osobowych przy użyciu poczty elektronicznej prywatnej, było wymagane szyfrowanie załączników (odrębne przesyłanie hasła – e-mail, sms, telefon, fax, list), a w temacie wiadomości zabronione używanie danych osobowych i informacji poufnych. Zabronione było też otwieranie wiadomości oraz załączników i linków od nieznanych nadawców, na wypadek cyberataków. Przetwarzanie danych mogło odbywać się w ramach udzielonego upoważnienia. Dopuszczając możliwość przesyłania informacji za pomocą prywatnej poczty elektronicznej podczas pracy zdalnej, przeprowadzono analizę zagrożeń, lecz nie udokumentowano jej wyników, a także nie określono rodzajów informacji przesyłanych tym kanałem.

Według Starosty, nieokreślenie rodzajów tych informacji wynikało z niezakładania żadnych ograniczeń w tym zakresie oraz wymogu szyfrowania przesyłanych plików, a także jednoczesnego zalecenia, aby korzystano przede wszystkim ze służbowych kont e-mail. Po aktualizacji PBI (zał. 13) praca zdalna była możliwa tylko i wyłącznie z wykorzystaniem programów i systemów udostępnionych przez Pracodawcę.

(akta kontroli str. 181, 195-196, 260, 296-306, 340-341, 388)

1.7. Zgodnie z § 20 ust. 2 pkt 13 KRI oraz w związku z PN-ISO/IEC 27001 (pkt A.16.1), w ramach SZBI/PBI określono zasady zarządzania incydentami związanymi z bezpieczeństwem informacji, wskazując warunki umożliwiające ich niezwłoczne zgłaszanie w ustalony sposób oraz szybkie podejmowanie działań korygujących, co zapewniało spójność i skuteczność zarządzania incydentami, z uwzględnieniem informowania o zdarzeniach i słabościach. Za szybką, skuteczną i zorganizowaną reakcję na ww. incydenty odpowiadał IOD jako administrator danych osobowych, który w myśl art. 33 RODO miał obowiązek zgłaszania naruszenia ochrony danych organowi nadzorczemu w ciągu 72 godz. W przypadku przekroczenia tego czasu, wymagane było dołączenie do zgłoszenia wyjaśnienia przyczyn opóźnienia. W razie małego prawdopodobieństwa wystąpienia ryzyka naruszenia praw i wolności osób fizycznych, można było odstąpić od zgłoszenia naruszenia. Jeżeli dotyczyło ono podmiotu przetwarzającego, to podmiot ten był zobowiązany zgłosić niezwłocznie incydent administratorowi danych. Zadaniem administratora było dokumentowanie wszelkich naruszeń, w tym ich okoliczności, ich skutków oraz podjętych działań zaradczych. W przypadku zgubienia lub kradzieży sprzętu, dokumentów lub innych nośników informacji, użytkownik miał obowiązek zgłosić niezwłocznie to zdarzenie pracodawcy oraz ASI i IOD.

(akta kontroli str. 20, 182)

W ramach regulacji dotyczących zarządzania incydentami (PBI) określono katalog zdarzeń, które należało traktować bezwzględnie jako wymagające zgłoszenia i podjęcia działań:

- sytuacje losowe lub oddziaływanie czynników zewnętrznych na zasoby systemu informatycznego, np. wybuch gazu, pożar, zalanie lub katastrofa budowlana, terroryzm, ingerencja ekipy remontowej, kradzież i napad;
- niewłaściwe parametry środowiska, np. wysoka wilgotność lub temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy i wibracje przemysłowe;
- awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych osobowych (sabotaż);
- pojawienie się odpowiedniego komunikatu alarmowego od części systemu zapewniającej ochronę zasobów lub inny komunikat o podobnym znaczeniu;
- pogorszenie jakości danych lub inne odstępstwo od stanu oczekiwanego, wskazujące na zakłócenia systemu albo jego niepożądaną modyfikację;

- naruszenie/próba naruszenia integralności systemu lub jego bazy danych oraz niedopuszczalna manipulacja danymi osobowymi;
- modyfikacja danych lub jej próba bez upoważnienia/autoryzacji albo istnienie nieautoryzowanych kont dostępu (tzw. „bocznej furtki");
- ujawnienie osobom nieuprawnionym danych osobowych/objętych tajemnicą, procedury ochrony przetwarzania lub innych elementów zabezpieczeń;
- nieprzypadkowe odstępstwa od zasad bezpieczeństwa pracy w systemie wskazujące na przełamanie lub zaniechanie ochrony danych (praca osoby nieuprawnionej, sygnał o uporczywym nieautoryzowanym logowaniu itp.);
- podmiana lub zniszczenie nośników z danymi osobowymi bez upoważnienia, skasowanie lub skopiowanie tych danych w sposób niedozwolony;
- naruszenie dyscypliny pracy/bezpieczeństwa informacji (niewylogowanie się, pozostawienie danych w drukarce, niewykonanie kopii bezpieczeństwa itp.).

(akta kontroli str. 25-27)

1.8. Zgodnie z § 20 ust. 2 pkt 8 KRI oraz w związku z sytuacją epidemiczną wskutek zagrożeń COVID-19, celem zapewnienia bezpiecznej pracy przy przetwarzaniu mobilnym i pracy na odległość, w Starostwie opracowano i wdrożono Regulamin wykonywania pracy w formie zdalnej i rotacyjnej[16], jako uzupełnienie do regulacji określonych w SZBI. Regulamin określał podstawowe obowiązki i warunki jakie powinien spełniać pracownik podczas pracy zdalnej i w systemie rotacyjnym (w tym bhp), warunki w jakich ta praca miała być wykonywana oraz zasady dotyczące bezpieczeństwa informacji, w tym korzystania z Internetu i urządzeń służących do pracy, sposobu postępowania z dokumentami papierowymi, metod zabezpieczania przekazywanych informacji i postępowania w sytuacjach szczególnych (np. awaria sprzętu lub oprogramowania, utrata sprzętu, dokumentów lub nośników). Regulamin zawierał wzory polecenia pracy zdalnej, wniosku o zgodę na pracę zdalną, informacji o czynnościach wykonywanych podczas pracy w tych formach oraz oświadczenia o zapoznaniu się pracownika z treścią tego regulaminu.

(akta kontroli str. 296-306)

Celem realizacji rozwiązań organizacyjnych określonych w Regulaminie, wdrożono następujące mechanizmy techniczne:

- usługę katalogową *Active Directory* pozwalającą na centralne zarządzanie konfiguracją stanowisk komputerowych i uprawnieniami[17] oraz wymuszanie zmiany haseł użytkowników stacji roboczych (sprawdzenia okresowe[18]),
- oprogramowanie antywirusowe do wykrywania i zapobiegania działalności szkodliwego oprogramowania na stacjach roboczych/serwerach,
- urządzenie UTM[19] filtrujące ruch wchodzący/ wychodzący z sieci LAN oraz serwer mechanizmu dostępu zdalnego VPN,
- oprogramowanie służące inwentaryzacji i monitorowaniu urządzeń w sieci urzędu, w tym ich konfiguracji, wydajności stacji roboczych i serwerów oraz identyfikacji zainstalowanego oprogramowania, a także umożliwiające połączenia zdalne (przejęcie pulpitu), skanowanie sieci oraz podgląd aktywności użytkowników (licencja, polisa serwisowa),
- oprogramowanie do tworzenia kopii zapasowych na stacjach roboczych (raporty z weryfikacji),

---

[16] Zarządzenie Starosty Nr 31/2020 z 16 października 2020 r. ws. określenia zasad pracy zdalnej i rotacyjnej – dalej: „Regulamin".

[17] Sprawdzenia okresowe wykonano 17 lipca 2020 r i 15 września 2021 r.

[18] Sprawdzenia wykonano 12 marca i 16 grudnia 2020 r. oraz 2 czerwca i 19 lipca 2021 r.

[19] Ang. *Unified threat management.*

- centralny UPS chroniący sieć teleinformatyczną przed uszkodzeniami wskutek utraty zasilania.

(akta kontroli str. 255-265, 351-375)

1.9. W myśl § 20 ust. 2 pkt 6 KRI, celem uświadomienia, kształcenia i szkolenia z zakresu bezpieczeństwa informacji, pracownicy Starostwa przeszli stosowne szkolenie nt. zasad bezpiecznej pracy zdalnej, które w formie instruktażu odbyło się w 2 października 2020 r. – jeden dzień po aktualizacji PBI w tym zakresie (zał. 13). Szkolenie w siedzibie Starostwa przeprowadzili IOD i ASI, prezentując zasady bezpiecznej pracy zdalnej, w tym procedury bezpieczeństwa przetwarzania danych, sieci domowej i stanowiska pracy, logowania i zdalnego dostępu do sieci służbowej, wykorzystania prywatnego sprzętu komputerowego i przechowywania danych.

Spośród 46 zatrudnionych pracowników, w szkoleniu wzięło udział 40 osób (wg listy obecności). Czterech pracowników zapoznało się z tematyką szkolenia w innym terminie[20], gdyż w dniu tego szkolenia przebywali na urlopach wypoczynkowych (dwie osoby), zwolnieniu lekarskim (jedna) oraz poza urzędem w celu prywatnym (jedna), jedna osoba nie odbyła szkolenia z powodu przebywania na zwolnieniu lekarskim i dotychczas urlopie rodzicielskim oraz jedna wskutek przebywania na urlopie wychowawczym (nadal). Zgodnie z PBI, poza pracownikami Starostwa szkoleniem wstępnym z zakresu ochrony danych osobowych zostali objęci m.in. praktykanci, stażyści, doradcy zawodowi, pisarze PKL[21] i inni specjaliści, tj. ogółem 42 osoby w 2020 r. i 10 osób w 2021 r.

(akta kontroli str. 138-143, 250, 324-329)

1.10. Stosownie do § 20 ust. 2 pkt 1 KRI oraz PN-ISO/IEC 27001, w Starostwie dokonywano aktualizacji regulacji wewnętrznych w zakresie ich przydatności, adekwatności i skuteczności w procesie zarządzania bezpieczeństwem informacji. Weryfikacja procedur SZBI (przegląd zasad), prowadzona w sposób ciągły wraz ze zmianami otoczenia, które wprowadzały nowe ryzyka dotyczące bezpieczeństwa informacji (w tym COVID-19), skutkowała wprowadzeniem zasad bezpiecznej pracy w systemach informatycznych podczas pracy zdalnej oraz modyfikacją wzoru karty szkolenia wstępnego w zakresie ochrony danych osobowych. W ramach tej modyfikacji określono katalog naruszeń lub uzasadnionych podejrzeń naruszenia ich zabezpieczenia. Od wprowadzenia SZBI w 2018 r., przegląd dokumentacji systemu odbywał się corocznie we wrześniu w latach następnych.

(akta kontroli str. 32, 36-41, 178-184, 251)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej obszarze nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK pozytywnie ocenia działania Starostwa w powyższym obszarze.

OBSZAR

2. Rozwiązania organizacyjne i techniczne mające na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej

Opis stanu faktycznego

2.1. Spośród 46 pracowników zatrudnionych w Starostwie w 2020 r. i 47 w 2021 r. (do 29 listopada), z uwzględnieniem zmian kadrowych, pracę zdalną wykonywało odpowiednio 42 i 47 osób na podstawie polecenia Pracodawcy oraz 10 i 12 osób na podstawie polecenia ze swego wniosku. Odnotowano także odpowiednio 15 i 11 przypadków świadczenia pracy zdalnej przez pracowników w okresie kwarantanny oraz sześć i dziewięć przypadków w czasie izolacji. Z grupy pracowników pracujących w systemie pracy zdalnej wyłączone były osoby długotrwale nieobecne

[20] Dwie osoby 5 października oraz po jednej osobie 30 października i 23 listopada 2020 r.

[21] Powiatowa Komisja Lekarska orzekająca o stanie zdrowia dla celów wojskowych.

wskutek przebywania na zwolnieniach lekarskich i urlopach, tj. trzech pracowników w 2020 r. i sześciu w 2021 r.

Z wyjaśnień Starosty wynikało, że pracowała ona w systemie zdalnym, lecz nie dokumentowała tego w formie polecenia tej pracy. Jako Pracodawca i kierownik jednostki organizowała jej pracę, a jednocześnie była przypisana do jednej z grup pracujących naprzemiennie. Podała, że jako osoba zarządzająca zakładem pracy nie podlegała obowiązkowi szczegółowego ewidencjonowania czasu pracy, lecz tylko ewidencji uproszczonej ograniczonej do oznaczania obecności i nieobecności.

(akta kontroli str. 330, 342-349)

2.2. Wszyscy pracownicy skierowani do pracy zdalnej zostali zapoznani z zasadami dotyczącymi zapewnienia bezpieczeństwa informacji w trakcie jej wykonywania. Wiedzę w tym zakresie nabyli poprzez udział w szkoleniu 2 października 2020 r. (w zakresie wg zał. nr 13 do PBI) oraz zapoznanie się z Regulaminem pracy zdalnej wprowadzonym przez Starostę 16 października 2020 r., w związku z zagrożeniem epidemicznym COVID-19. Wdrożenie Regulaminu pozostawało w gestii naczelników wydziałów oraz pracowników na samodzielnych stanowiskach, w tym IOD i ASI. Na podstawie art. 3 ustawy o zapobieganiu, przeciwdziałaniu i zwalczaniu epidemii[22], wdrożono formę wykonywania pracy, określonej w umowie o pracę lub umowie cywilnoprawnej, w systemie zdalnym, tj. poza miejscem stałego wykonywania, ze wskazaniem adresu i terminu oraz zgodą na osobiste stawienia się w urzędzie w nieprzewidzianych i nagłych przypadkach, po wcześniejszym uzgodnieniu. Pracę zdalną wykonywano na podstawie pisemnego polecenia lub na wniosek pracownika, a w razie potrzeby pracy rotacyjnej, naprzemiennie w domu i w urzędzie, pracownik wypełniał formularz jej polecenia podając jej terminy. Na polecenie pracodawcy pracownik miał obowiązek składania pisemnej informacji z wykonanych zdalnie czynności, podając ich datę, godziny pracy i zakres. Do polecenia lub wniosku o umożliwienie pracy zdalnej pracownik musiał dołączyć w formie pisemnej lub elektronicznej oświadczenie o zapoznaniu się z Regulaminem i był zobowiązany do przestrzegania RODO i PBI.

W zakresie organizacji pracy zdalnej/rotacyjnej Starosta wyjaśniła, że pracownicy w tym systemie pracowali w okresie od 19 października 2020 r. do 14 maja 2021 r. Przy organizacji tej pracy zastosowano podział pracowników na dwie niezależne grupy pracujące naprzemiennie według ustalonych harmonogramów, co pozwalało ograniczać rozprzestrzenianie COVID-19 w przypadku zakażeń wśród pracowników oraz ich izolację wobec epidemii, nie wpływając na ciągłość funkcjonowania urzędu.

(akta kontroli str. 296-306, 342-349)

2.3. Liczba pracowników Starostwa wykonujących pracę zdalną z wykorzystaniem sprzętu zapewnionego przez pracodawcę (laptopy) wyniosła 11 osób w 2020 r. oraz 22 w 2021 r. (stan na 20 października), zaś korzystających ze sprzętu prywatnego (laptopy) – odpowiednio 16 i dziewięć osób, a 19 i 14 osób korzystało z prywatnych telefonów (tylko do komunikacji głosowej). Pracownicy nie korzystali ze służbowych telefonów i nośników danych. Starosta polecając pracę zdalną określała, że osoba pracująca w tym trybie jest zobowiązana do pracy wg swego zakresu obowiązków, wykonywanych dotąd w ramach umowy o pracę/ cywilnoprawnej, z uwzględnieniem Regulaminu i sytuacji epidemicznej. Spośród odpowiednio 11 i 22 osób pracujących zdalnie z użyciem powierzonego im sprzętu komputerowego, wszystkie miały dostęp do systemów teleinformatycznych urzędu poprzez program z pakietem biurowym i pocztę elektroniczną. Dostęp ten był realizowany za pośrednictwem mechanizmu

[22] Ustawa z 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych i wywołanych nimi sytuacji kryzysowych (Dz. U. poz. 1842 ze zm.).

VPN oraz pulpitu zdalnego, w sposób uniemożliwiający współdzielenie schowka systemowego oraz korzystanie z dysków i drukarek urzędu.

Badanie dokumentacji dotyczącej pracy zdalnej pięciu pracowników[23], którzy pracowali wykorzystując komputery służbowe, wykazało, że konfiguracja tego sprzętu i infrastruktury urzędu zapewniała pełną realizację zadań służbowych przez tych pracowników. Pracownicy pracujący zdalnie posiadali dostęp do zasobów informatycznych urzędu jako tzw. zwykli użytkownicy, tj. na poziomie uprawnień adekwatnych do swoich zadań, zaś uprawnienia administratora posiadał tylko ASI.

Starosta wyjaśniła, że pracownicy skierowani do pracy zdalnej oraz wyposażeni w komputery służbowe mogli realizować obowiązki służbowe w pełnym zakresie, a ograniczenie wiązało się jedynie z niemożliwością wytwarzania dokumentów tradycyjnych (papierowych) w miejscu wykonywania pracy zdalnej, ponieważ nie wydawano im służbowych drukarek. Ograniczono również kontakty telefoniczne z petentami i nie dokonywano przekierowania telefonów służbowych pracowników na ich prywatne numery. Wskutek niemożliwości wcześniejszego przewidzenia rozmiaru zapotrzebowania na sprzęt komputerowy do pracy zdalnej oraz zaplanowanie środków budżetowych na jego zakup, w miarę posiadanych środków podejmowano działania w zakresie zapewnienia jego wystarczającej liczby.

(akta kontroli str. 331-336, 342-349)

2.4. W komputerach udostępnianych przez pracodawcę do wykonywania pracy zdalnej stosowano mechanizmy umożliwiające zapewnienie odpowiedniego poziomu bezpieczeństwa zarówno systemów i oprogramowania oraz przetwarzania danych. Oględziny pięciu komputerów przenośnych (laptopów) udostępnionych do pracy zdalnej wykazały, że stosowano w nich poziom uprawnień nie niższy od tych, które zapewniały realizację zadań w trybie pracy biurowej. Poprzez zastosowanie w tych komputerach zapory systemowej, legalnego oprogramowania i aktualnego programu antywirusowego, stosowanie szyfrowania kanałów łączności i uwierzytelnianie logowania silnym hasłem (wymogi PBI), osoby pracujące zdalnie zapewniły w pełni bezpieczne i skuteczne funkcjonowanie urzędu, co potwierdziły także wyjaśnienia Starosty. Zabezpieczając informacje przed utratą lub zniszczeniem, sporządzano kopie danych przechowywanych i przetwarzanych na urządzeniach poza urzędem. Oględziny kont użytkowników potwierdziły, że listy grup, których byli oni członkami, nie wykraczały poza nadany im poziom uprawnień.

(akta kontroli str. 337-339, 342-350)

2.5. Zgodnie z Regulaminem, celem zapewnienia ciągłości funkcjonowania urzędu, Pracodawca dopuścił możliwość pracy w systemie zdalnym przez pracowników, z wykorzystaniem komputerów prywatnych. Określił w tym celu minimalne wymogi dla prywatnego sprzętu i oprogramowania, w myśl których pracownicy zobowiązali się zorganizować stanowisko pracy zdalnej w sposób zapewniający jej bezpieczne i higieniczne warunki, w tym przestrzegać obowiązujących przepisów RODO, zasad SZBI oraz kontrolować i uniemożliwić dostęp osób trzecich do używanego sprzętu i posiadanych informacji (PBI). Uzależnił pracę zdalną od spełniania podstawowych zasad bezpieczeństwa, w tym posiadania legalnego oprogramowania, aktualnego systemu bezpieczeństwa i programu antywirusowego. Komputer prywatny musiał posiadać możliwość wielopoziomowego uwierzytelniania[24] oraz silne hasło dostępu. W ramach używania tego sprzętu dopuszczono korzystanie ze służbowej poczty elektronicznej i zapewniono możliwość jej szyfrowania oraz tworzenia i edycji dokumentów. W odniesieniu do minimalnych wymagań (PBI), celem zapewnienia

[23] Doboru dokonano celowo według osądu kontrolera.

[24] Autoryzacja następowała przynajmniej trzyetapowo, tj. od posiadania danych autoryzacyjnych na komputerze prywatnym, poprzez uwierzytelnienie się do aplikacji VPN, a następnie autoryzację na pulpicie zdalnym za pomocą usługi *Active Directory*.

bezpieczeństwa informacji, ASI dokonywał przeglądów tych komputerów zdalnie, odnotowując to w odpowiednim rejestrze.

Badanie dokumentacji pięciu pracowników[25], którzy pracowali zdalnie wykorzystując komputery prywatne, wykazało, że stosowane zasady zapewniały poufność informacji, w tym danych osobowych i innych tajemnic prawnie chronionych, których ujawnienie mogłoby narazić interes Pracodawcy na szkodę oraz zapewniało wykonanie wszystkich zadań służbowych przez pracowników, a tym samym ciągłość działania urzędu. Pracownicy korzystający z tych komputerów zostali zobowiązani do postępowania zgodnie z procedurami bezpiecznego przetwarzania informacji. Po zakończeniu pracy informacje te były każdorazowo przenoszone automatycznie do zasobów jednostki jako kopie zapasowe, nie pozostając w pamięci ww. komputerów.

Z uwagi na bezpieczeństwo informacji pracownicy korzystali tylko ze służbowej poczty elektronicznej. W ramach minimalnych wymagań w zakresie bezpieczeństwa przetwarzanych informacji na komputerach prywatnych sprawdzano legalność i aktualność ich oprogramowania, posiadanie programu antywirusowego, włączenie zapory systemowej, technikę logowania do systemu i tworzenia haseł oraz możliwość automatycznego blokowania urządzenia po dłuższej nieaktywności.

(akta kontroli str. 178-183, 296-301, 336-339, 342-349)

2.6. Zgodnie z wymogami PN-ISO/IEC 27001 (pkt A.11.2), urząd zapobiegał utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów i zakłóceniom działania, gdyż osoby wykonujące pracę zdalną nie pobierały z urzędu oryginałów i kserokopii dokumentów, lecz korzystały z ich skanów (do wglądu) za pomocą elektronicznego systemu obiegu dokumentów, po uzyskaniu zdalnego dostępu do sieci urzędu. W PBI zawarto w tym celu zakaz zabierania dokumentów lub ich kopii poza siedzibę Pracodawcy. W przypadku niezbędnej potrzeby, za zgodą naczelnika wydziału, osoba pracująca zdalnie mogła skopiować dane dokumenty (wg listy), a po ich wykorzystaniu była zobowiązana je zwrócić, przy czym ich kompletność podlegała weryfikacji przez naczelnika. Z kontroli wynikało jednak, że z uwagi na dostęp pracowników do zasobów (aktywów) jednostki poprzez pulpit zdalny, nie zachodziła potrzeba korzystania z dokumentów w formie papierowej, a dla potrzeb służbowych były te dokumenty przeglądane w ramach systemu ich elektronicznego obiegu.

(akta kontroli str. 182, 342-349)

2.7. Z wyjaśnień Starosty wynikało, że monitorowanie i nadzór pracy zdalnej, w tym zagadnień dotyczących bezpieczeństwa informacji, oparte było ma mechanizmach mających na celu ograniczanie dostępu pracowników jedynie do zasobów, które były im niezbędne do wykonywania obowiązków służbowych. Pomocą ku temu była aplikacja *Active Directory*. Dzięki wdrożonym rozwiązaniom, automatycznie była nadzorowana złożoność haseł dostępowych do komputerów oraz czas ich ważności, a także wymuszana zmiana tych haseł w odpowiednim czasie, co zapobiegało instalacji nieautoryzowanego oprogramowania (ograniczenie uprawnień). W ramach nadzoru dokonywano aktualizacji oprogramowania użytkowego i antywirusowego i innych zabezpieczeń, zaś poprzez zastosowanie blokady wykorzystania pamięci przenośnych i schowka pulpitu zdalnego oraz mapowania dysków i drukarek lokalnych zapobiegano potencjalnym wyciekom informacji *(IT Manager)*. Starosta podała, że była w stałym kontakcie telefonicznym przede wszystkim z naczelnikami wydziałów, ale także zlecała osobiście zadania pracownikom. Praktyka ta wykazała, że żadne polecenia nie były bagatelizowane, a pracownicy przekazywali terminowo informacje (telefoniczne/pisemne) o wykonaniu poleceń, a decyzje, postanowienia, akty prawne i inne sprawy realizowano z zachowaniem terminów i poszanowaniem Kodeksu pracy. Możliwości Pracodawcy w celu zapobiegania rozprzestrzenianiu się

[25] Dobór celowy jw.

choroby COVID-19 oraz wewnętrzne regulacje wz. pracy zdalnej były wystarczające do prawidłowego realizowania zadań służbowych. Mimo trudności wynikających z warunków epidemicznych, w Starostwie zachowano jakość i ciągłość jego pracy, zachowując bezpieczeństwo przetwarzanych i przechowywanych informacji oraz zachowano standardy i terminy prowadzonych postępowań. Dzięki bieżącej analizie warunków pracy zdalnej, aktualizacji zasad i wprowadzaniu regulacji adekwatnych do potrzeb, urząd zagwarantował pełne bezpieczeństwo zasobów informatycznych oraz prawidłowość i skuteczność działania.

(akta kontroli str. 342-349)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej obszarze nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

NIK pozytywnie ocenia działania Starostwa w powyższym obszarze.

IV. Uwagi i wnioski

Najwyższa Izba Kontroli, w związku z niestwierdzeniem nieprawidłowości, nie formułuje uwag i wniosków.

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 Olsztynie. 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.

Olsztyn, 29 listopada 2021 r.

Najwyższa Izba Kontroli
Delegatura w Olsztynie

Kontroler
Edward Odojewski
Główny specjalista kontroli państwowej

podpis

Dyrektor
z up. Piotr Wanic
Wicedyrektor

podpis