NAJWYŻSZA IZBA KONTROLI
Delegatura w Olsztynie

LOL.410.017.05.2021

Jan Zbigniew Nadolny
Starosta Powiatu Bartoszyckiego
ul. Grota Roweckiego 1
11-200 Bartoszyce

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 Bartoszycach (dalej: „Starostwo" lub "Urząd")
Kierownik jednostki kontrolowanej	Jan Zbigniew Nadolny – Starosta Powiatu Bartoszyckiego od 22 listopada 2018 r.
Zakres przedmiotowy kontroli	1. Organizacja bezpieczeństwa informacji. 2. Wdrożone i stosowane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji w pracy zdalnej.
Okres objęty kontrolą	Lata 2020-2021 (do 26 listopada), 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[1]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Delegatura w Olsztynie
Kontroler	Rafał Dmytrenko, specjalista kontroli państwowej, upoważnienie do kontroli nr LOL/119/2021 z 10 października 2021 r.

(akta kontroli str. 1-2)

II. Ocena ogólna[2] kontrolowanej działalności

OCENA OGÓLNA

W okresie objętym kontrolą w Urzędzie podejmowano działania na rzecz zapewnienia bezpieczeństwa informacji, w tym w pracy na odległość i mobilnym przetwarzaniu danych. Dotyczyły jednak one przede wszystkim danych osobowych. Wszystkim pracownikom administracyjnym Urzędu przypisano w zakresach czynności pracowniczych odpowiedzialność za ochronę danych osobowych, pracownicy merytoryczni Urzędu potwierdzili zapoznanie z treścią Polityki Ochrony Danych Osobowych. Starosta wypełnił wymóg z art. 37 ust. 1 Rozporządzenia 679/2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[3] powołując Inspektorów Ochrony Danych w Starostwie. W Urzędzie prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych według wzoru określonego w załączniku nr 9 do PODO.

W PODO z 2020 r. zawarto procedurę. „Praca zdalna z wykorzystaniem służbowego i prywatnego sprzętu do zadań służbowych oraz pracy z dokumentacją papierową". Zgodnie z tą procedurą, do przetwarzania danych osobowych poza obszarem przetwarzania Administrator mógł dopuszczać osoby posiadające pisemne upoważnienia do pracy na nośnikach służbowych lub prywatnych i na kserokopiach dokumentacji służbowej i które to osoby złożyły oświadczenia o zapoznaniu się z zasadami pracy zdalnej oraz stosowaniu się do zasad określonych w PODO. W toku kontroli stwierdzono, że Administrator Danych Osobowych stosował

[1] Dz. U. z 2020 r. poz. 1200, ze zm., dalej: ustawa o NIK.

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

[3] Dz. U.UE.L.2016.119.1, dalej: RODO.

opracowane i ustanowione zasady wobec osób wykonujących pracę zdalną zawarte w PODO. Stosowano także rozwiązania techniczne i technologiczne podnoszące poziom bezpieczeństwa przetwarzanych informacji. Pracownicy zatrudnieni w Starostwie, wykonujący pracę zdalną w latach 2020/2021 potwierdzili w formie oświadczenia zapoznanie się z zasadami ochrony danych osobowych podczas pracy zdalnej zawartymi w PODO

W kontrolowanym okresie nie dokonywano przeglądów PODO i tym samym nie modyfikowano zawartych w nich procedur.

W toku kontroli stwierdzono też nieprawidłowości, które dotyczyły:

- nieopracowania, nieustanowienia i niewdrożenia w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji[4] (w tym Polityki Bezpieczeństwa Informacji[5]), stosownie do przepisów 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[6], obejmujących swoim zakresem wszystkie kategorie przetwarzanych w Urzędzie informacji,
- nierealizowania niektórych zadań określonych w zasadach pracy zdalnej z wykorzystaniem sprzętu komputerowego, tj. monitorowania ruchu sieciowego pod kątem wystąpienia niepożądanych połączeń oraz włączania i konfigurowania zapory sieciowej w celu uniemożliwienia podłączenia komputera do niezabezpieczonych sieci Wi-Fi.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[7] kontrolowanej działalności

OBSZAR

1. Organizacja bezpieczeństwa informacji

Opis stanu faktycznego

1.1 Do 26 listopada 2021 r., tj. dnia zakończenia kontroli, w Urzędzie nie opracowano i nie wdrożono SZBI (w tym nie wprowadzono PBI), spełniającego wymogi określone przepisami § 20 ust. 2 rozporządzenia KRI, do czego zobowiązywał § 20 ust. 1 ww. rozporządzenia. Zagadnienie to opisano w sekcji „Stwierdzone nieprawidłowości".

W okresie objętym kontrolą w Starostwie funkcjonowały dwie Polityki Ochrony Danych Osobowych („PODO") wprowadzone zarządzeniami Starosty, pierwsza z 25 listopada 2019 r. i druga z 9 listopada 2020 r. Polityki te były jedynymi dokumentami określającymi zasady i reguły dotyczące bezpieczeństwa informacji. Oba dokumenty określały zakres ich stosowania ograniczony do danych osobowych.

(akta kontroli str.3-52,190-193)

PODO z 2019 r. opracowana była przez inspektora ochrony danych będącego pracownikiem firmy zewnętrznej świadczącej usługi na podstawie umowy pomiędzy nią a Starostą. Zawierała ona podstawowe zagadnienia dotyczące ochrony danych osobowych określone wymaganiami RODO.

(akta kontroli str.3-28,53-55)

[4] Dalej: SZBI.
[5] Dalej: PBI.
[6] Dz.U. z 2017 r., poz. 2247, dalej: rozporządzenie KRI.
[7] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

W PODO z 2020 r. opracowanej przez inną firmę zewnętrzną określono zasady wynikające z Polskiej Normy PN-ISO/IEC 27001, dotyczące zarządzania uprawnieniami użytkowników, wynoszenia aktywów (sprzęt, nośniki, oryginały dokumentów, kopie dokumentów), bezpieczeństwa sprzętu i aktywów poza siedzibą, pozostawiania sprzętu bez opieki, zabezpieczenia przed szkodliwym oprogramowaniem, zabezpieczenia sieci, przesyłania informacji, zabezpieczenia wiadomości w formie elektronicznej oraz zarządzania incydentami związanymi z bezpieczeństwem informacji. Zgodnie z określonym w Polityce zakresem stosowania zasady te miały zastosowanie do danych osobowych przetwarzanych w Urzędzie.

(akta kontroli str.28-52,56-66,174-176,177-189)

1.2 Wszystkim pracownikom administracyjnym Urzędu przypisano w zakresach czynności pracowniczych odpowiedzialność za ochronę danych osobowych. Wśród obowiązków Głównego Specjalisty Informatyka wyszczególniono także przestrzeganie instrukcji w sprawie zarządzania systemem informacyjnym służącym przetwarzaniu danych osobowych, instrukcji postępowania w przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego oraz zabezpieczenie przestrzegania prawa autorskiego i ochrony danych osobowych przy używaniu oprogramowania informatycznego w Starostwie. W Urzędzie prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych według wzoru określonego w załączniku nr 9 do PODO.

(akta kontroli str. 68-75,166-173,215-220)

1.3 Starosta w formie zarządzenia w dniu 2 lipca 2019 r. powołał Inspektora Ochrony Danych („IOD") w Starostwie, który pełnił tę funkcję do 2 lipca 2020 r. IOD posiadał certyfikat potwierdzony Egzaminem Kompetencyjnym IOD poświadczający kwalifikacje w zakresie pełnienia swojej funkcji. Na mocy umowy zlecenia zawartej pomiędzy Starostwem a IOD, w ww. dniu IOD przypisano zadania o których mowa w art. 39 RODO, tj.:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia RODO[8] oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
- monitorowanie przestrzegania rozporządzenia RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35,
- współpraca z Prezesem Urzędu Ochrony Danych Osobowych,
- pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

Ponadto, zobowiązano Inspektora do pełnienia roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia RODO.

(akta kontroli str.53-55,76-85)

[8] Dz. Urz. UE L 119, s.1).

Starosta 3 lipca 2020 r. zawarł umowę o wykonywanie zadań IOD z innym podmiotem niż dotychczas i zarządzeniem z 10 lipca 2020 r. wyznaczył nowego IOD – pracownika ww. firmy. Posiadał on certyfikat wystawiony przez Centrum Bezpieczeństwa Informatycznego zaświadczający ukończenie szkolenia doskonalącego „Zasady i bezpieczeństwo przetwarzania informacji, ze szczególnym uwzględnieniem danych osobowych".

Zakres zadań powierzonych IOD wyczerpywał katalog określony w art. 39 RODO. Ponadto IOD był zobowiązany m.in. do analizy i weryfikacji opracowanych rejestrów czynności przetwarzania danych oraz rejestru kategorii czynności przetwarzania danych osobowych, opracowywania procedur zgłaszania ewentualnych naruszeń ochrony danych osobowych oraz kontaktu z organami nadzorczymi i wykonywania analizy i modyfikacji zapisów w umowach powierzenia przetwarzania danych osobowych pod kątem zgodności z wymogami art. 28 RODO.

(akta kontroli str.56-66,86-91,153-165)

1.4 W PODO z 2020 r. zawarto procedurę „Praca zdalna z wykorzystaniem służbowego i prywatnego sprzętu do zadań służbowych oraz pracy z dokumentacją papierową" (Załącznik nr 14 do Polityki), stanowiącą uszczegółowienie zasad ogólnych zawartych z PODO. Określono w niej także zasady postępowania z nośnikami, tj. m.in.:

- odpowiedzialność za przygotowanie upoważnień do pracy na nośnikach służbowych/prywatnych i kserokopii dokumentacji służbowej,
- ustalono jakie dokumenty w formie papierowej mogły być wynoszone przez pracownika poza jednostkę (nie dotyczyło to dokumentów sklasyfikowanych jako informacje niejawne),
- zasady niszczenia wydruków technicznych lub błędnie wykonanych w miejscu pracy zdalnej, przy czym rekomendowanym rozwiązaniem było gromadzenie takich wydruków w jednym miejscu i zniszczenie ich po powrocie do pracy,
- obowiązek szyfrowania dysków twardych, nośników danych lub kart pamięci, na których były gromadzone informacje służbowe,
- rodzaje dokumentów jakie mogły być drukowane lub skanowane na sprzęcie prywatnym lub zapewnienie odpowiedniego sprzętu pracownikowi – rekomendowanym rozwiązaniem był całkowity zakaz wykonywania takich operacji.

(akta kontroli str. 29-52,177-189)

1.5 W ramach PODO z 2020 r., w Załączniku nr 14 dotyczącym pracy zdalnej ustalono, że dopuszczalne było wykonywanie pracy zdalnej z wykorzystaniem służbowego sprzętu oraz pracy z dokumentacją papierową przy zachowaniu określonych w procedurze zasad. Do zadań Administratora należało m.in:

- przygotowanie protokołu zdawczo-odbiorczego sprzętu służbowego do wykonywania pracy zdalnej,
- zatwierdzanie upoważnienia do pracy na nośnikach służbowych i kserokopii dokumentacji służbowej i wpisywanie do ewidencji nadanych upoważnień,
- przekazywanie pracownikowi komputera służbowego do pracy zdalnej przygotowanego wcześniej przez pion informatyki,
- wymaganie od pracownika aby w przypadku dokumentacji papierowej wydruki i dokumentacja były niedostępne dla osób postronnych i pozostawione bez nadzoru pracownika.

Do obowiązków Administratora Systemu Informatycznego należały działania dotyczące bezpieczeństwa sprzętu i innych aktywów poza terenem Starostwa w zakresie m.in.:

- zainstalowania i zaktualizowania programu antywirusowego,
- zaktualizowania systemu operacyjnego na komputerze,
- ustawienia hasła do logowania do komputera zgodnego z przyjętą polityką haseł,
- przygotowania i skonfigurowania komputera, aby logował się do zabezpieczonej i odpowiednio skonfigurowanej sieci VPN.

(akta kontroli str. 29-52,177-189)

1.6 W Załączniku nr 14 do PODO określono, że komputery używane do pracy zdalnej musiały być przygotowane i skonfigurowane tak, aby użytkownik logował się tylko do zabezpieczonej sieci VPN, miały posiadać zainstalowany i skonfigurowany program antywirusowy, zaktualizowany system operacyjny, a ustawione hasła do logowania się do komputera musiały być zgodne z przyjętą polityką haseł.

W PODO określono zasadę, że w przypadku używania do pracy zdalnej komputerów prywatnych do zadań służbowych można było korzystać tylko ze służbowej poczty e-mail. Przed wysłaniem wiadomości należało się upewnić, że była wysłana do właściwego adresata oraz zabroniono otwierania wiadomości pochodzących od nieznanych nadawców. W przypadku przesyłania plików lub dokumentów za pomocą służbowej poczty elektronicznej należało każdorazowo zabezpieczać je hasłem (hasło należało przekazywać innym kanałem kontaktowym).

(akta kontroli str. 29-52,177-189)

Zgodnie z wyjaśnieniem Administratora Systemu Informatycznego, w Urzędzie nie dopuszczono możliwości korzystania z prywatnych kont pocztowych, w związku z tym nie zachodziła potrzeba stosowania dodatkowych zabezpieczeń wysyłanych wiadomości.

(akta kontroli str.92-93)

1.7 W myśl zapisów PODO użytkownik, który stwierdził lub podejrzewał fakt naruszenia danych osobowych był zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu, który zgłaszał fakt naruszenia Administratorowi i IOD. Użytkownik, który stwierdził fakt naruszenia danych osobowych miał obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn i skutków naruszenia. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należało zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia IOD lub innej osoby upoważnionej przez Administratora.

IOD zobowiązany był do udokumentowania przypadku naruszenia bezpieczeństwa danych sporządzając raport, zasięgając potrzebnych mu opinii i proponując działania naprawcze w rejestrze naruszeń i incydentów ochrony danych osobowych zawierającym także wskazanie działań korygujących i zapobiegawczych.

W przypadku naruszenia ochrony danych osobowych Administrator bez zbędnej zwłoki maksymalnie. po 72 godzinach po stwierdzeniu naruszenia miał obowiązek zgłaszać ten fakt Urzędowi ochrony danych.

Jeżeli naruszenie ochrony danych osobowych mogło powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zobowiązany był do zawiadomienia osoby, której to dotyczyło.

(akta kontroli str. 29-52,177-189)

1.8 W okresie objętym kontrolą zasady dotyczące przetwarzania danych osobowych poza obszarem przetwarzania ujęte były w procedurze pracy zdalnej zawartej w PODO. Administrator mógł dopuszczać osoby posiadające pisemne upoważnienia do pracy na nośnikach służbowych lub prywatnych i kserokopii dokumentacji służbowej oraz te, które złożyły oświadczenia o zapoznaniu się z zasadami pracy zdalnej oraz stosowaniu się do zasad określonych w Załączniku nr 14 do PODO.

Administrator określił podstawowe warunki i obowiązki, jakie miał spełniać pracownik. W procedurze określono zadania polegające m.in. na:

- zapewnieniu sobie w miejscu pracy przestrzeni, odpowiedniej do tego, aby osoby postronne nie miały dostępu do informacji służbowych,
- nie pozostawianiu komputera używanego do pracy zdalnej bez nadzoru, a w przypadku krótkotrwałego opuszczenia stanowiska pracy zablokowanie go i zabezpieczenie dokumentów,
- używaniu do logowania się na komputerze haseł zgodnych z polityką haseł przyjętych w Urzędzie,
- używaniu tylko rekomendowanych przez administratora przeglądarek internetowych,
- nie instalowaniu żadnego oprogramowania bez uprzedniej konsultacji z pionem informatyki,
- nie logowaniu się prywatnym komputerem do publicznych sieci Wi-Fi,
- odpowiednim zabezpieczeniu przed dostępem osób trzecich drukowanych na służbowym sprzęcie dokumentów,
- zabezpieczaniu wydruków technicznych lub błędnie wykonanych do momentu powrotu do pracy, a następnie niszczenie ich w niszczarce,
- każdorazowym zabezpieczaniu hasłem plików lub dokumentów wysyłanych za pomocą poczty email.

(akta kontroli str.29-52,177-189)

1.9 W Urzędzie w 2021 r. przeprowadzono dla 58 pracowników jedno szkolenie w zakresie bezpieczeństwa informacji p.t. „Praktyczne aspekty stosowania Polityki Ochrony Danych Osobowych w kontekście zagrożeń związanych z kradzieżą lub wyłudzeniem danych osobowych".

Zgodnie z wymaganiami określonymi w PODO pracownicy merytoryczni Urzędu potwierdzili zapoznanie się z jej treścią (na załączniku nr 20 do PODO).

(akta kontroli str.124,174-176)

1.10 W kontrolowanym okresie nie dokonywano przeglądów PODO i tym samym nie modyfikowano procedur zawartych w PODO.

Starosta wyjaśnił, że aktualnie nie ma obowiązku wykonania przeglądu i aktualizacji wdrożonej polityki bezpieczeństwa informacji PODO, ale zaplanowano już na grudzień 2021 r. audyt bezpieczeństwa Urzędu, którego elementem jest przegląd i aktualizacja polityki PODO.

W 2020 r. IOD dokonał analizy poziomu ryzyka bezpieczeństwa w procesach przetwarzania danych osobowych realizowanych w Starostwie.

(akta kontroli str.94-123,194-213)

Stwierdzone nieprawidłowości

W Urzędzie nie opracowano, nie ustanowiono i nie wdrożono SZBI, o którym mowa w § 20 ust. 1 rozporządzenia KRI. Nie opracowano i nie wdrożono PBI, rozumianej jako zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa, według których dana organizacja zarządza i udostępnia swoje zasoby informacji.

Zgodnie z ww. przepisem jednostki realizujące zadania publiczne mają obowiązek opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia SZBI zapewniającego poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Wymagania dotyczące opracowania SZBI uznaje się za spełnione, jeżeli został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001 (§ 20 ust. 3 ww. rozporządzenia), a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie związanych z tą normą innych Polskich Norm, w tym: PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem; PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

W 2019 r. w Urzędzie sporządzono wykaz zbiorów danych osobowych (Załącznik nr 1 do PODO z 2019 r.), ale jak określono w nazwie zawierał jedynie zbiory, które identyfikowano pod kątem zawartych w nich danych osobowych. Inwentaryzacja zasobów informacyjnych powinna obejmować wszystkich rodzaje informacji przetwarzanych w Urzędzie, zgodnie z wymaganiami Polskiej Normy PN-ISO/IEC 27001 (Załącznik nr 4: Wzorcowy wykaz celów stosowanych zabezpieczeń, pkt A.8.2. Klasyfikacja informacji), gdzie określono m.in., że „informacja powinna być klasyfikowana z uwzględnieniem wymogów prawnych, wartości, krytyczności i wrażliwości na nieuprawnione ujawnienie lub modyfikację."

Zasady i kwestie podstawowe w PODO z 2019 r. oraz zakres stosowania polityki zawarty w PODO z 2020 r. potwierdziły, że regulacje dotyczące bezpieczeństwa informacyjnego Urzędu odnosiły się tylko i wyłącznie do danych osobowych.

Starosta wyjaśnił, że dokumentacja zawarta w PODO określa zasady i reguły dotyczące bezpieczeństwa przetwarzania informacji danych osobowych w sposób kompleksowy i jej zasady mogą zostać rozszerzone do ich stosowania w ogólnym pojęciu przetwarzania informacji służbowej i jego zdaniem jest wystarczająca do odpowiedniego zabezpieczenia przetwarzanych informacji przez pracowników wyznaczonych do pracy zdalnej.

Zdaniem NIK, ograniczając zakres stosowania ww. polityk do danych osobowych nie spełniono jednak w pełni wymogu wynikającego z § 20 ust. 1 rozporządzenia KRI nakładającego na jednostki realizujące zadania publiczne obowiązek opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

OCENA CZĄSTKOWA

W okresie objętym kontrolą w Urzędzie funkcjonowały dwie Polityki Ochrony Danych Osobowych („PODO") z 2019 r. i 2020 r., będące dokumentami określającymi zasady i reguły dotyczące bezpieczeństwa informacji. Określony w nich zakres stosowania dotyczył danych osobowych. Wszystkim pracownikom administracyjnym Urzędu przypisano w zakresach czynności pracowniczych odpowiedzialność za ochronę danych osobowych, pracownicy merytoryczni Urzędu potwierdzili zapoznanie się z treścią PODO. Starosta wypełnił wymóg z art. 37 ust. 1 RODO powołując Inspektorów Ochrony Danych w Starostwie. W Urzędzie prowadzona była ewidencja osób upoważnionych do przetwarzania danych osobowych według wzoru określonego w Załączniku nr 9 do PODO. W PODO z 2020 r. zawarto procedurę „Praca zdalna z wykorzystaniem służbowego i prywatnego sprzętu do zadań

służbowych oraz pracy z dokumentacją papierową". Jednakże w Urzędzie ograniczono system bezpieczeństwa informacji do przyjęcia Polityk Ochrony Danych Osobowych.

OBSZAR

2. Wdrożone i stosowane rozwiązania organizacyjne i techniczne mające na celu zapewnienie bezpieczeństwa informacji w pracy zdalnej

Opis stanu faktycznego

2.1 W okresie objętym kontrolą pracę zdalną na podstawie polecenia pracy zdalnej wykonywało z inicjatywy pracodawcy 56 pracowników w 2020 r. i 38 w 2021 r. (wg stanu na dzień 29 października 2021 r.). Nie wystąpiły przypadki polecenia pracy zdalnej z wniosku pracownika. W czasie kwarantanny w 2020 r. pracę zdalną wykonywało dziewięciu pracowników, a w 2021 r. sześciu pracowników, w czasie izolacji taką pracę wykonywało pięciu pracowników w 2021 r., w 2020 r. nie było takich przypadków.

(akta kontroli str.125)

2.2 56 pracowników zatrudnionych w Starostwie, wykonujących pracę zdalną w latach 2020/2021 potwierdziło w formie oświadczenia zapoznanie się z zasadami ochrony informacji podczas pracy zdalnej zawartymi w PODO. Dotyczyło to pracowników wykorzystujących następujące zasoby:

- praca z dokumentacją papierową – 40 osób,
- praca z wykorzystaniem komputerów prywatnych – 13 osób,
- praca z wykorzystaniem komputerów służbowych – 3 osoby.

Pracownicy zadeklarowali znajomość zasad ochrony danych osobowych w zakładzie pracy i zobowiązali się do stosowania ich w pracy zdalnej. PODO zawierało zapis o dopuszczalności pracy zdalnej tylko wtedy, gdy zastosowane były zasady bezpieczeństwa oraz zabezpieczenia wskazane w procedurze pracy zdalnej zawartej w PODO.

(akta kontroli str.126-127,128)

2.3 W okresie objętym kontrolą wśród pracowników wykonujących pracę zdalną z wykorzystaniem sprzętu zapewnionego przez pracodawcę w 2020 r., wykonywały dwie osoby za pomocą komputera służbowego, 11 osób przy pomocy telefonu służbowego tylko do komunikacji głosowej. Do pracy zdalnej z wykorzystaniem sprzętu prywatnego skierowano 12 pracowników wykorzystujących komputer prywatny i 27 pracowników używających telefonów prywatnych tylko do komunikacji głosowej.

W 2021 r. do pracy zdalnej z wykorzystaniem sprzętu zapewnionego przez pracodawcę skierowano trzy osoby korzystające z komputera służbowego i dziewięć osób używających telefonu służbowego tylko do komunikacji głosowej. W tym okresie 12 pracowników skierowanych do pracy zdalnej wykorzystywało komputery prywatne, a 24 pracowników używało telefonów prywatnych tylko do komunikacji głosowej.

(akta kontroli str.128)

2.4 W Urzędzie w okresie objętym kontrolą trzech pracowników używało komputerów służbowych do pracy zdalnej. Komputery te były przekazane na podstawie protokołu zdawczo-odbiorczego stanowiącego załącznik nr 1 do procedury zawartej w załączniku Nr 14 do PODO.

Według oświadczeń dwóch z nich, komputery były wykorzystywane wyłącznie do uruchamiania za pośrednictwem łącza VPN usług zdalnego pulpitu ich komputerów stacjonarnych, znajdujących się w budynku Starostwa.

Według oświadczenia Administratora systemu informatycznego, który był użytkownikiem trzeciego komputera laptopy służbowe zostały przygotowane do zdalnej pracy m.in. poprzez:

- sprawdzenie czy system operacyjny był wspierany przez producenta i ewentualne zaktualizowanie go,
- zainstalowanie programu antywirusowego,
- ustawienie hasła do logowania do komputera,
- skonfigurowanie bezpiecznego łącza VPN dostępowego do sieci Starostwa, ograniczonego wyłącznie do usług zdalnego pulpitu do swojego służbowego stacjonarnego komputera.

Ponadto, jak oświadczył Administrator, pracownicy zostali przeszkoleni w zakresie bezpieczeństwa pracy zdalnej oraz sposobu korzystania z dostępu do systemów i programów Starostwa.

(akta kontroli str.128-131,149-152)

W wyniku przeprowadzonych w toku kontroli oględzin laptopów służbowych używanych do pracy zdalnej stwierdzono, że:

- komputery przygotowano i skonfigurowano do logowania się do zabezpieczonej sieci VPN,
- wyłączono możliwość dostępu do BIOS komputera poprzez zabezpieczenie go hasłem oraz wyłączono w BIOS możliwości boot'owania z innych nośników niż dysk twardy,
- zawierały zainstalowany program antywirusowy, który był skonfigurowany w taki sposób, aby bazy wirusów aktualizowały się samoczynnie,
- ustawiono automatyczne aktualizacje systemu operacyjnego,
- konta użytkowników nie należały do grupy administratorzy,
- logowanie do komputera wymagało wpisania hasła,
- każdy z komputerów był przyporządkowany jednemu pracownikowi Urzędu.

(akta kontroli str.132-137)

W okresie objętym kontrolą Urząd nie realizował m.in. następujących zadań określonych w PODO w zakresie pracy zdalnej z wykorzystaniem służbowego sprzętu do zadań służbowych:

- szyfrowania dysków twardych, nośników danych lub kart pamięci, na których znajdowały się dane,
- blokowania możliwości instalacji sprzętu zewnętrznego,
- włączenia i skonfigurowania firewall w celu uniemożliwienia podłączenia komputera pracownika do niezabezpieczonych sieci Wi-Fi,
- aktualizowania oprogramowania serwera poczty e-mail oraz monitorowania ruchu na serwerze.

Starosta wyjaśnił, że dane nie były przetwarzane na dyskach lokalnych komputerów przeznaczonych do pracy zdalnej i nie było potrzeby szyfrowania nośników pamięci oraz blokowania możliwości instalacji urządzeń zewnętrznych. Dodał, że urząd nie miał możliwości monitorowania serwera poczty, ponieważ nie jest przez urząd zarządzany. Zagadnienie to opisano w sekcji „stwierdzone nieprawidłowości".

(akta kontroli str. 29-52,177-189,190-193)

2.5 W okresie objętym kontrolą 13 pracowników używało komputerów prywatnych do pracy zdalnej. Na podstawie oświadczeń pięciu pracowników wybranych w sposób losowy spośród pracujących zdalnie użytkowników ustalono, że

użytkowali oni laptopów prywatnych przystosowanych przez Urząd do wykonywania pracy zdalnej. Zgodnie z oświadczeniami użytkowników komputery zostały skonfigurowane przez Administratora systemu informatycznego m.in. w następujący sposób:

- zaktualizowano system operacyjny i ustawiono automatyczną aktualizację,
- zabezpieczono programem antywirusowym,
- dostęp do komputera został zabezpieczony hasłem oraz ustawiono wygaszacz ekranu, który do odblokowania wymagał wpisania hasła,
- skonfigurowano bezpieczne połączenie z siecią komputerową Starostwa umożliwiające podłączenie się do komputera w Urzędzie za pomocą zdalnego pulpitu autoryzowanego hasłem.

Według oświadczenia Administratora systemu informatycznego komputery prywatne pracowników Urzędu zostały przygotowane do zdalnej pracy po uprzednim zaleceniu użytkownikom nie wytwarzania informacji na prywatnym komputerze, przeszkoleniu użytkowników w zakresie bezpieczeństwa pracy zdalnej oraz sposobu korzystania z dostępu do systemów i programów Starostwa. Ustalono również zasady i sposób kontaktu w przypadku problemów technicznych.

Jak oświadczył Administrator po wyrażeniu zgody przez pracowników komputer prywatny został przygotowany przez obsługę informatyczną poprzez:

- sprawdzenie czy system operacyjny jest wspierany przez producenta i ewentualne zaktualizowanie tego systemy operacyjnego,
- zainstalowanie programu antywirusowego i przeskanowanie na obecność złośliwego oprogramowania,
- ustawienie hasła logowania zgodnego z polityką haseł do komputera oraz ustawienie wygaszacza ekranu zabezpieczonego hasłem,
- skonfigurowanie bezpiecznego łącza VPN dostępowego do sieci Starostwa, ograniczonego wyłącznie do usług zdalnego pulpitu do swojego służbowego stacjonarnego komputera w budynku Starostwa, który był zabezpieczony hasłem użytkownika zgodnym z polityką haseł.

Ww. ustawienia sprawiły, że wszystkie operacje i dostępy do systemów Starostwa wykonywane były poprzez komputer pracujący w budynku Starostwa Powiatowego w Bartoszycach.

(akta kontroli str.128,138-143,149-152)

W okresie objętym kontrolą, spośród zadań określonych w PODO, w zakresie pracy zdalnej z wykorzystaniem prywatnego sprzętu do zadań służbowych Urząd nie realizował m.in.:

- monitorowania ruchu sieciowego pod kątem wystąpienia niepożądanego ruchu,
- włączania i skonfigurowania firewall w celu uniemożliwienia podłączenia komputera pracownika do niezabezpieczonych sieci Wi-Fi,
- określenia maksymalnej wielkości pliku, który można przesłać na wspólny zasób,
- w przypadku braku zgody na ingerencję w prywatny sprzęt pracownika – przekazania mu minimalnych wymagań, jakie musi spełnić pracownik oraz jego sprzęt oraz poinformowania go o zakazie logowania się do systemów dziedzinowych Urzędu.

Starosta wyjaśnił, że pracownicy pracowali na założonym koncie dostępu do służbowego komputera, który nie był w grupie administratorzy. Nie było ustalonego wspólnego zasobu do wspólnej komunikacji, więc wielkość pliku nie była określana.

Starosta dodał, że wszyscy pracownicy delegowani do pracy zdalnej na prywatnym sprzęcie wyrazili zgodę na odpowiedną ingerencję w swój sprzęt w celu zabezpieczenia komputera do pracy zdalnej. Nie było przypadku nie spełnienia wymagań komputera prywatnego wykorzystywanego do pracy zdalnej.

(akta kontroli str. 29-52,177-189,190-193)

2.6 Pracę zdalną z dokumentacją papierową zawierającą dane osobowe regulowała w sposób ogólny procedura zawarta w Załączniku Nr 14 do PODO. Określono w niej środki ostrożności polegające na uniemożliwieniu osobom postronnym przeglądania wydruków i dokumentacji bez nadzoru pracownika Urzędu oraz niszczeniu za pomocą niszczarki na bieżąco nieprzydatnych dokumentów.

Z analizy losowej próby pięciu oświadczeń złożonych przez pracowników Urzędu wynikało m.in., że byli oni poinformowani o sposobie zabezpieczania dokumentów w pracy zdalnej oraz że dokumenty były chronione przed dostępem osób trzecich poprzez odpowiedni nadzór w czasie pracy i odpowiednie ich przechowywanie po zakończonej pracy. Niepotrzebne i nieprzydatne wydruki były niszczone. Dokumentacja była przekazana pracownikom na podstawie protokołu zdawczo – odbiorczego zawartego w Załączniku Nr 14 do PODO z adnotacją „dokumenty zabezpieczone w zasznurowanych teczkach i segregatorach przekazano pracownikom do wykonywania niezbędnych zadań".

Starosta wyjaśnił, że w dokumentacji dotyczącej bezpieczeństwa informacji nie ma bezpośrednio wskazanych kategorii dokumentów wynoszonych do pracy zdalnej. Nadmienił, że każdy pracownik pobierał dokumentację w zależności od wydziału i swojego stanowiska pracy, czyli były to w przypadku Urzędu dokumenty z wydziału geodezji tzw. operaty, z wydziału finansowego - dokumenty księgowe, a z wydziału architektury i budownictwa – projekty budowlane.

(akta kontroli str. 144-148,177-189,194-213)

2.7 Urząd w okresie objętym kontrolą nie monitorował i nie nadzorował pracy zdalnej prowadzonej, zarówno na sprzęcie służbowym i prywatnym w kontekście bezpieczeństwa informacji.

Jak wyjaśnił Starosta, w Urzędzie nie było narzędzi informatycznych umożliwiających monitorowanie czynności pracownika podczas pracy zdalnej na komputerze w kontekście bezpieczeństwa informacji. Starosta dodał, że monitorowanie i nadzór pracowników nad wykonywaniem pracy zdalnej polegał na sprawdzaniu pracowników poprzez kontakt telefoniczny bezpośrednich przełożonych oraz kierownictwa Starostwa. Ponadto informatyk Starostwa miał możliwości sprawdzenia czasu połączenia komputera zdalnego z urzędem.

(akta kontroli str.177--214)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono nieprawidłowość polegającą na nierealizowaniu przez obsługę informatyczną niektórych zadań określonych w zasadach pracy zdalnej z wykorzystaniem sprzętu komputerowego, tj. monitorowania ruchu sieciowego pod kątem wystąpienia niepożądanych połączeń, włączania i konfigurowania zapory sieciowej w celu uniemożliwienia podłączenia komputera pracownika do niezabezpieczonych sieci Wi-Fi.

Starosta wyjaśnił, że każdy pracownik podczas pracy zdalnej podłączał komputer do swojej domowej sieci Wi-Fi i nie było potrzeby łączenia z obcą niezabezpieczoną siecią Wi-Fi. Dodał, że nie posiada narzędzi umożliwiających monitorowanie pod katem niepożądanego ruchu sieciowego, a komputery pracy zdalnej łączyły się z urzędem za pomocą usługi VPN, która umożliwiała jako jedyny ruch sieciowy protokół dostępu do pulpitu zdalnego, blokując jakikolwiek inny rodzaj połączeń.

Zdaniem NIK jednak, obowiązek wykonywania określonych w PODO zadań nie był warunkowany szczególnymi okolicznościami, a zatem powinny być one realizowane w pełni.

OCENA CZĄSTKOWA

Administrator stosował opracowane i ustanowione zasady wobec osób wykonujących pracę zdalną zawarte w PODO. Natomiast rozwiązania techniczne i technologiczne służące zapewnieniu odpowiedniego poziomu bezpieczeństwa przetwarzanych informacji określone w PODO stosowano nie w pełnym zakresie. Pracownicy zatrudnieni w Starostwie wykonujących pracę zdalną w okresie objętym kontrolą potwierdzili w formie oświadczenia zapoznanie się z zasadami ochrony danych osobowych podczas pracy zdalnej zawartymi w PODO.

IV. Uwagi i wnioski

Najwyższa Izba Kontroli nie formułuje uwag. W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Zrealizowanie wymogu wynikającego z rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności nakładającego na jednostki realizujące zadania publiczne obowiązek opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.
2. Realizowanie zadań wymaganych w procedurach zawartych w PODO.

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.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 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.

Olsztyn, 30 listopada 2021 r.

Kontroler
Rafał Dmytrenko
specjalista kontroli państwowej

.....
podpis

Delegatura w Olsztynie
Dyrektor
z up.
Piotr Wanic
Wicedyrektor

.....
podpis