Bydgoszcz, 24 października 2018 r.

WOJEWODA KUJAWSKO-POMORSKI
WNK.III.431.1.3.2018.GL.

Pan
Jerzy Rabeszko
Wójt Gminy Stolno
Stolno 112
86-212 Stolno

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 16 ust. 2 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1] oraz art. 25 ust. 1 pkt 3a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[2] (dalej: ustawa o informatyzacji) w Gminie Stolno, Stolno 112, 86-212 Stolno, w dniach: 21-23 sierpnia 2018 r. Wojewoda Kujawsko-Pomorski przeprowadził kontrolę prawidłowości zrealizowaną przez starszego inspektora wojewódzkiego, nr upoważnienia 495/2018 w zakresie:
1. przedmiot kontroli: wykorzystywanie systemów teleinformatycznych do realizacji zadań publicznych.
2. okres objęty kontrolą: od 1 stycznia 2017 r. do dnia rozpoczęcia kontroli.

W wyniku przeprowadzonej kontroli kontrolowaną działalność jednostki ocenia się pozytywnie z nieprawidłowościami.

Dokonana ocena została oparta o następującą skalę ocen:
- pozytywna,
- pozytywna z uchybieniami,
- pozytywna z nieprawidłowością,
- pozytywna z nieprawidłowościami,
- negatywna (po przekroczeniu przyjętego progu istotności).

Kontrolę przeprowadzono w poniższych obszarach.

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.
W ramach tego obszaru poddano kontroli:
1.1. Usługi elektroniczne;
1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE);

[1] Dz.U. Nr 185, poz. 1092.
[2] Dz. U. z 2017 r. poz. 570, ze zm.

1.3. Model usługowy;
1.4. Współpracę systemów teleinformatycznych z innymi systemami;
1.5. Obieg dokumentów w podmiocie publicznym;
1.6. Formaty danych udostępniane przez systemy teleinformatyczne.

2. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.
W ramach tego obszaru poddano kontroli:
2.1. Dokumenty z zakresu bezpieczeństwa informacji;
2.2. Analizę zagrożeń związanych z przetwarzaniem informacji;
2.3. Inwentaryzację sprzętu i oprogramowania informatycznego;
2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych;
2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji;
2.6. Pracę na odległość i mobilne przetwarzanie danych;
2.7. Serwis sprzętu informatycznego i oprogramowania;
2.8. Procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji (dalej także: BI);
2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji;
2.10. Kopie zapasowe;
2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych;
2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji;
2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych;
2.14. Rozliczalność działań w systemach informatycznych.

3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych.

Oceny dokonano na podstawie poniższych ustaleń.

1. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami.

1.1. Usługi elektroniczne.

Podmiot kontrolowany udostępnia elektroniczną skrzynkę podawczą, zgodnie z art. 16 ust. 1a ustawy o informatyzacji.

Obecnie na stronie BIP Gminy Stolno znajduje się odesłanie do dwóch usług elektronicznych, tj. *Pismo ogólne do podmiotu publicznego* oraz *Wniosek o wydanie dowodu osobistego*. Ponadto podmiot prowadzi punkt potwierdzania Profilu zaufanego. Jak oświadczył Wójt, Gmina obecnie jest na etapie realizacji projektu dofinansowanego z UE, w ramach którego zostanie uruchomionych 10 nowych usług.

Na stronie BIP Gminy Stolno znajduje się odesłanie do opisów usług, które zawierają wymagane informacje dotyczące m.in. aktualnej podstawy prawnej świadczonych usług, nazwy usług, miejsca świadczenia usług (złożenia dokumentów), terminu składania i załatwiania spraw oraz nazwy komórek odpowiedzialnych za załatwienie spraw, zgodnie z § 5 ust. 2 pkt 1 i 4 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[3] (dalej: rozporządzenie KRI).

1.2. Centralne repozytorium wzorów dokumentów elektronicznych.

Zgodnie z art. 19 b ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[4] organy administracji publicznej przekazują

[3] Dz. U. z 2016 r. poz. 113
[4] Dz. U. z 2017 r. poz. 570, ze zm.

do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. W związku z tym, że Urząd Gminy Stolno nie opracował i nie udostępniał usług elektronicznych w CRWDE do tej pory nie przekazano do Centralnego Repozytorium Wzorów Dokumentów Elektronicznych żadnych procedur. Jak wynika ze złożonych wyjaśnień oraz przedłożonych dokumentów planowane wdrożenie 10 nowych usług będzie wiązało się z przekazaniem stosownych wzorów do CRWDE.

1.3. Model usługowy.
W podmiocie kontrolowanym nie istnieją wewnętrzne procedury dotyczące obsługi usług elektronicznych oraz monitoringu dotyczącego dostarczania ich na zadeklarowanym poziomie. Stanowi to naruszenie § 15 ust. 2 rozporządzenia KRI, w którym jest mowa o tym, że zarządzanie usługami realizowanymi przez systemy teleinformatyczne odbywa się w oparciu o udokumentowane procedury. Tym samym nie ma możliwości zweryfikowania sposobu realizacji tych procedur.

1.4. Współpraca systemów teleinformatycznych z innymi systemami.
Kwestie współpracy systemów teleinformatycznych z innymi systemami regulują § 5 ust. 3 pkt 3 oraz § 16 ust. 1 rozporządzenia KRI.
Systemy teleinformatyczne w Urzędzie, tj. Źródło oraz CEIDG funkcjonują na zasadzie dwustronnej komunikacji. Podlegają one ciągłej modyfikacji i aktualizacjom. Zdolność kontrolowanych systemów do współpracy z innymi systemami lub rejestrami publicznymi utrzymywana jest po stronie podmiotu kontrolowanego poprzez dostosowywanie oprogramowania do współpracy z systemami w związku z ich zmianami, aktualizacjami. Po stronie podmiotu zapewnia się, zgodnie ze złożonymi przez Wójta wyjaśnieniami, dbanie o bezpieczne i niezawodne działanie sprzętu, spełnianie wymogów i parametrów sprzętowych, co podmiot kwalifikuje jako działania skuteczne z uwagi na fakt, że stosowane oprogramowanie oraz sprzęt współpracują z systemami.
Podmiot zawarł 27 września 2016 r. umowę dotyczącą budowy, utrzymania, i udostępniania strony Biuletynu Informacji Publicznej i jest to jedyny system, za którego parametry odpowiada Gmina.

1.5. Obieg dokumentów w podmiocie publicznym.
Do zagadnienia obiegu dokumentów odnosi się § 20 ust. 2 pkt 9 rozporządzenia KRI.
W podmiocie kontrolowanym stosuje się system EZD jako system wspomagający. Podstawową formą obiegu dokumentów jest forma papierowa.
Dokumenty wewnętrzne, jakie regulują zarządzanie dokumentacją to:
- Zarządzenie Nr 43/2017 Wójta Gminy Stolno z dnia 11 kwietnia 2017 roku w sprawie Regulaminu Organizacyjnego Urzędu Gminy Stolno;
- Zarządzenie Nr 59/2013Wójta Gminy Stolno z dnia 16 lipca 2013 r. w sprawie ustalenia szczegółowych zasad wykonywania czynności kancelaryjnych, w tym oznaczeń pism stanowiących znak sprawy oraz skrótów stosowanych przy dekretowaniu pism ze zmianami;
- Zarządzenie Nr 127/2014 Wójta Gminy Stolno z dnia 31 grudnia 2014 r. w sprawie wprowadzenia instrukcji ustalającej zasady sporządzania, obiegu i kontroli oraz przechowywania i zabezpieczania dokumentów księgowych i ksiąg rachunkowych w Urzędzie Gminy Stolno;
- Instrukcja obsługi systemu EZD.

Ponadto obieg dokumentów regulowany jest rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów

zakładowych.[5]

1.6. Formaty danych udostępniane przez systemy teleinformatyczne.
Omawiany obszar reguluje § 17 ust. 1 oraz § 18 ust. 1-2 rozporządzenia KRI.
Kodowanie znaków w dokumentach wysyłanych lub odbieranych przez podmiot kontrolowany odbywa się według standardu Unicode UTF-8.
Udostępnianie zasobów informatycznych z systemów teleinformatycznych podmiotu publicznego, określone w § 18 ust. 1 rozporządzenia KRI, możliwe jest w Urzędzie Gminy Stolno w przypadku plików o rozszerzeniach: .pdf, .doc, .rtf, .odt, .xls, .docx, .xlsx, .jpg, .mp3, .avi, .zip.
Przyjmowanie dokumentów elektronicznych, określone w § 18 ust. 2 rozporządzenia KRI, możliwe jest w Urzędzie Gminy Stolno w przypadku plików o rozszerzeniach .pdf, .doc, .rtf, .odt., .xls, .docx, .xlsx, .jpg, .mp3, .avi, .zip, .dwg, .dxf.
Są to formaty danych określone w załączniku nr 2 lub 3 do rozporządzenia KRI. Tym samym spełnione są wymagania określone ww. przepisach. Jak wyjaśnił Wójt, wszystkie pliki z ww. rozszerzeniami można otworzyć za pomocą ogólnodostępnego darmowego oprogramowania. Jednakże Gmina posiada kilka licencji na oprogramowanie MS Office, dzięki czemu możliwe jest otworzenie plików z ww. rozszerzeniami w wersjach bardziej złożonych niż podstawowe.

2. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.
2.1. Dokumenty z zakresu bezpieczeństwa informacji.
W zakres dokumentów stanowiących System zarządzania bezpieczeństwem informacji (dalej: SZBI) wchodzą:
a) wprowadzone zarządzeniem Nr 2/2016 z dnia 4 stycznia 2016 r. Wójta Gminy Stolno w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych w Urzędzie Gminy Stolno:
- Polityka bezpieczeństwa Informacji w Urzędzie Gminy Stolno;
- Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.
b) zarządzenie Nr 50/2018 Wójta Gminy Stolno z dnia 11 maja 2018 r. w sprawie wprowadzenia polityki ochrony danych w Urzędzie Gminy Stolno.
c) zarządzenie Nr 66/2015 Wójta Gminy Stolno z dnia 7 lipca 2015 r. w sprawie wprowadzenia planu ochrony informacji niejawnych dla Urzędu Gminy Stolno.
d) zarządzenie Nr 53/2018 Wójta Gminy Stolno z dnia 23 maja 2018 r. w sprawie kontroli nadzoru nad ruchem osobowym w Urzędzie Gminy Stolno.
e) Metodyka szacowania ryzyka dla Urzędu Gminy Stolno zatwierdzona wz. Wójta przez zastępcę wójta 27 kwietnia 2018 r.
Istnienie powyższych dokumentów wypełnia wymagania określone w § 20 ust. 1 rozporządzenia KRI odnoszące się do opracowania, ustanowienia, wdrożenia SZBI.
Z kolei wypełnienie obowiązku wynikającego z § 20 ust. 2 pkt 1 rozporządzenia KRI dotyczącego aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia realizowane jest poprzez coroczne opracowywanie planu audytu oraz sprawozdania z audytu.
Należy zauważyć, że Polityka bezpieczeństwa informacji w Urzędzie Gminy Stolno ogranicza się w swoich regulacjach do kwestii bezpieczeństwa przetwarzania danych osobowych pomijając aspekt bezpieczeństwa przetwarzania wszelkich innych informacji jakimi dysponuje podmiot kontrolowany. Ta sama uwaga dotyczy Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityki ochrony danych

[5] Dz. U. z 2011 r. nr 14 poz. 67, ze zm.

w Urzędzie Gminy Stolno. W związku z powyższym należy poddać pod rozwagę z jednej strony modyfikację wszystkich kluczowych dokumentów odnoszących się do bezpieczeństwa informacji, a z drugiej przeanalizować możliwość skonsolidowania w jednym akcie dublujących się rozwiązań prawnych. Będzie to sprzyjało ich przejrzystości i zwiększało możliwości ich praktycznego wykorzystania. Powyższa sugestia wynika również z faktu stwierdzenia sprzeczności pomiędzy aktami obowiązującymi w kontrolowanej jednostce. Gwoli przykładu można wskazać na przepis zawarty w Instrukcji zarządzania systemem informatycznym, gdzie na jego czwartej stronie w zakresie „Procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu" w ustępie 5 wskazano, że monitory komputerów wyposażone są we włączające się po 10 minutach od przerwania pracy wygaszacze ekranu. Z kolei w Polityce ochrony danych w Urzędzie Gminy Stolno na stronie 15 w części zatytułowanej „Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu" w punkcie 2 ustalono, że na stacjach roboczych oraz laptopach stosuje się wygaszacze ekranów aktywujące się po 5 minutach od momentu braku aktywności w systemie informatycznym.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji.
Regulacje wewnętrzne odnoszące się do zarządzania ryzykiem Bezpieczeństwa Informacji ujęte są w Metodyce szacowania ryzyka dla Urzędu Gminy Stolno. Dokument ten stanowi element realizacji obowiązku wynikającego z § 20 ust. 2 pkt 3 rozporządzenia KRI zobowiązującego do przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz do podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.
Zgodnie z wyjaśnieniami Wójta i otrzymaną dokumentacją w jednostce jest przeprowadzana okresowa analiza ryzyka utraty integralności, poufności lub dostępności informacji.
Skuteczność zarządzania bezpieczeństwem informacji przetwarzanych w systemach teleinformatycznych, w tym dostępność, autentyczność, poufność, niezawodność i integralność przetwarzanych danych reguluje Polityka ochrony danych, Polityka bezpieczeństwa informacji oraz Zarządzenie w sprawie kontroli nadzoru nad ruchem osobowym w Urzędzie Gminy Stolno. Zagrożenia związane z przetwarzaniem informacji są ograniczane m.in. poprzez politykę haseł wynikającą z ww. dokumentów, stosowanie zabezpieczeń programowych (oprogramowanie zabezpieczające i antywirusowe) i sprzętowo-technicznych (wszystkie pomieszczenia znajdują się w sieci alarmowej, która jest pod stałym monitoringiem firmy ochroniarskiej). Sposób postępowania w przypadkach naruszenia ochrony danych osobowych opisuje Polityka ochrony danych w Urzędzie Gminy Stolno w § 7.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego.
Przepis § 20 ust. 2 pkt 2 rozporządzenia KRI, zobowiązuje do utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Funkcję rejestru zasobów informatycznych pełni obecnie oprogramowanie Axence nVision, które umożliwia kontrolę nad infrastrukturą IT, prowadzenie listy zainstalowanego/używanego oprogramowania, usprawnienie zarządzania stacjami roboczymi oraz łatwiejsze planowanie nowych zakupów, a także ewidencję środków trwałych IT. Ponadto taka inwentaryzacja, zgodnie z wyjaśnieniami Wójta, prowadzona jest również corocznie w formie papierowej.
Przydzielanie, zwrot sprzętu i oprogramowania odbywa się zgodnie z Polityką bezpieczeństwa informacji i Polityką ochrony danych. Administrator systemu nadaje nowemu użytkownikowi (pracownikowi) uprawnienia dostępu do systemu. Ponadto pracownik/użytkownik otrzymuje stosowne upoważnienie do przetwarzania danych

osobowych. W praktyce przydzielanie i zwrot sprzętu i oprogramowania odbywa się w oparciu o bieżące potrzeby - w razie zmian kadrowych lub zmian wynikających ze zużycia sprzętu i wystąpienia nieodwracalnych awarii.

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych.
Obowiązek wynikający z § 20 ust. 2 pkt 4 rozporządzenia KRI dotyczy podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji.
Uprawnienia administratora zasobów IT w Urzędzie Gminy posiada pracownik zatrudniony na stanowisku ds. administrowania siecią informatyczną, zamówień publicznych i pozyskiwania funduszy unijnych.
Procedura odbierania/nadawania uprawnień w przypadku rotacji kadrowych, zmian zakresów wykonywanych obowiązków odbywa się zgodnie z Polityką ochrony danych i Instrukcją zarządzania systemem informatycznym. Z kolei § 20 ust. 2 pkt 5 rozporządzenia KRI zobowiązuje do bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób uczestniczących w procesie przetwarzania informacji. Zgodnie z przedłożonymi dokumentami w okresie kontrolowanym czterem osobom nadano upoważnienia uprawniające do pracy na określonych zbiorach danych. Czterem osobom natomiast cofnięto upoważnienia. *Zaznaczyć należy, że zakres upoważnień obejmuje tylko obszar danych osobowych bez uwzględnienia wszelkich innych informacji z jakimi pracownik ma styczność w toku wykonywania obowiązków.*

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.
Regulacje wewnętrzne dotyczące przeprowadzania szkoleń użytkowników zaangażowanych w procesy przetwarzania informacji w systemach teleinformatycznych znajdują się w Polityce bezpieczeństwa informacji oraz w Polityce ochrony danych w Urzędzie Gminy Stolno. *Przy czym odnoszą się one do szkoleń dotyczących przetwarzania danych osobowych, a nie wszystkich informacji przetwarzanych przez kontrolowany podmiot.*
W kontrolowanym okresie odbyło się pięć szkoleń związanych z obszarem kontroli.
Tematyka szkoleń nie wyczerpuje zakresu wskazanego w § 20 ust. 2 pkt 6 rozporządzenia KRI, zgodnie z którym w ramach szkolenia należy uwzględnić takie zagadnienia jak:
a) zagrożenia bezpieczeństwa informacji,
b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

2.6. Praca na odległość i mobilne przetwarzanie danych.
Wymóg wynikający z § 20 ust. 2 pkt 8 rozporządzenia KRI odnosi się do konieczności ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. Wymóg ten jest spełniony dzięki zawarciu wspomnianych zasad w Polityce bezpieczeństwa informacji, Instrukcji zarządzania systemem informatycznym oraz Polityce ochrony danych w Urzędzie Gminy Stolno. Istniejące zabezpieczenia opierają się m.in. na obowiązku stosowania haseł i numerów PIN.

2.7. Serwis sprzętu informatycznego i oprogramowania.
Jak wynika z wyjaśnień, Urząd nie posiada regulacji wewnętrznych, w których określono zasady współpracy z podmiotami zewnętrznymi w zakresie serwisu i rozwoju systemów teleinformatycznych, w tym klauzule prawne dotyczące BI, wymagane zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI. Urząd posiada natomiast podpisaną umowę serwisową z firmą

zewnętrzną (umowa nr 03/17 z 2 stycznia 2017 r.). Umowa zawiera zobowiązanie wykonawcy do przystąpienia do naprawy w nieprzekraczalnym terminie 48 godzin roboczych od zgłoszenia. Ponadto Gmina ma zagwarantowane prawo kontroli właściwego przetwarzania przez wykonawcę powierzonych danych osobowych. Natomiast zgodnie z § 20 ust. 2 pkt 10 rozporządzenia KRI, w umowach serwisowych podpisanych ze stronami trzecimi powinny znajdować się zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. *Brak jest w umowie zobowiązania wykonawcy do zachowania w tajemnicy/nieudostępniania wszelkich informacji jakie pozyska w związku z realizacją umowy.*
Regulacje wewnętrzne odnoszące się do wykonywania przeglądów i konserwacji systemu znajdują się w Instrukcji zarządzania systemem informatycznym oraz w Polityce ochrony danych w Urzędzie Gminy Stolno.

2.8. Procedury zgłaszania incydentów naruszenia BI.
W jednostce wprowadzono regulacje wewnętrzne określone w § 20 ust. 2 pkt 13 rozporządzenia KRI, tj. dotyczące zgłaszania incydentów naruszenia bezpieczeństwa informacji. Procedury zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji zostały zawarte w Instrukcji zarządzania systemem informatycznym oraz w Polityce ochrony danych w Urzędzie Gminy Stolno.
Ze złożonych wyjaśnień wynika, że w kontrolowanym okresie nie doszło do incydentów naruszenia bezpieczeństwa informacji.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji.
Audyty wewnętrzne obejmujące kwestie związane z bezpieczeństwem informacji są cyklicznie przeprowadzane, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.
Jak wyjaśnił Wójt Gminy Stolno wyniki audytów wykorzystuje się w celu sprawdzenia stopnia zabezpieczeń i stopnia stosowania wymogów określonych w PBI oraz w Polityce ochrony danych.

2.10. Kopie zapasowe.
Regulacje prawa powszechnie obowiązującego odnoszące się do sporządzania kopii zapasowych znajdują się w § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI, mówiącego o konieczności minimalizowania ryzyka utraty informacji w wyniku awarii.
Regulacje wewnętrzne dotyczące tworzenia kopii zapasowych znajdują się w Instrukcji zarządzania systemem informatycznym oraz w Polityce ochrony danych w Urzędzie Gminy Stolno. *Jednostka nie posiada dokumentacji potwierdzającej wykonywanie, przechowywanie i testowanie kopii zapasowych.*

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych.
Zgodnie ze złożonymi wyjaśnieniami zapewnienie funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności systemów informatycznych odbywa się poprzez zgłaszanie producentowi błędów w działaniu systemu, przekazywanie do producentów oprogramowania sugestii co do nowych funkcjonalności systemu mogących ułatwić jego pracę, niezawodność, zwiększenie wydajności itp. Systemy posiadają swoją kopię/kopie bazy, co daje możliwość łatwego ich przeniesienia i uruchomienia na innym sprzęcie.

W Urzędzie Gminy Stolno nie stworzono sformalizowanych procedur w zakresie projektowania systemów teleinformatycznych dotyczących architektury systemu, sposobu licencjonowania i wykorzystania praw autorskich, zgodności z obowiązującym prawem (m.in. z ustawą o informatyzacji), sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, zastosowania rozwiązań funkcjonalnych odpowiednich

dla osiągniecia założonych celów, prezentacji treści dla osób niepełnosprawnych, wydajności, poziomu niezawodności, w tym parametrów SLA na usługi serwisowe, mechanizmów kontroli i audytu. Przy czym systemy teleinformatyczne (Źródło, CEIDG) zostały dopuszczone do użytkowania. Aplikacja Źródło oraz CEIDG są systemami udostępnionymi przez odpowiednie ministerstwa sprawujące nadzór nad aplikacjami. System BIP natomiast, jak wyjaśnił Wójt Gminy Stolno, spełnia wszystkie standardy i wymogi określone w przepisach, a w szczególności w ustawie o dostępie do informacji publicznej[6] oraz w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej[7].

W jednostce brak jest również regulacji wewnętrznych opisujących wymagania w zakresie wdrażania systemów teleinformatycznych, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji a także warunków i kryteriów odbioru oraz regulacji wewnętrznych opisujących sposób przeprowadzania zmian w systemach teleinformatycznych (w trakcie ich eksploatacji), w tym opisu: zgłaszania zmiany, analizy zmiany pod kątem wykonalności, kosztów, ryzyk, a także określenia sposobu wykonania i odbioru zmiany.

Jednocześnie brak jest regulacji wewnętrznych opisujących proces monitorowania systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności w celu zapobieżenia ewentualnym problemom z tym związanym.

Niemniej funkcjonuje oprogramowanie Axence nVision, które umożliwia monitorowanie. Oprogramowanie umożliwia prowadzenie kompleksowej kontroli nad infrastrukturą IT, a także pełnej listy zainstalowanego/używanego oprogramowania. Oprogramowanie w sposób kompleksowy wpływa na podniesienie poziomu bezpieczeństwa i ograniczenie wystąpienia zagrożeń w całym systemie teleinformatycznym.

W kontrolowanym okresie nie wdrażano nowych systemów teleinformatycznych, zmiany w funkcjonujących systemach dokonywane są automatycznie przez organy udostępniające te systemy.

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji.

Regulacje prawa powszechnie obowiązującego odnoszące się do ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami znajdują się w § 20 ust. 2 pkt 7, 9, 11 rozporządzenia KRI.

Regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji określono w Polityce bezpieczeństwa informacji oraz w Polityce ochrony danych.

W celu monitorowania działań użytkowników w systemie w Urzędzie funkcjonuje system Axence nVision umożliwiający monitorowanie działań użytkowników. Umożliwia ponadto blokowanie niebezpiecznych domen WWW przed przypadkowym wejściem i pobraniem złośliwego oprogramowania.

Zgodnie ze złożonymi wyjaśnieniami loga systemowe sprawdzane są doraźnie i wyrywkowo.

W zakresie zabezpieczenia techniczno-organizacyjnego w odniesieniu do pomieszczenia serwerowni wymienić należy zapewnienie w tym pomieszczeniu odpowiedniej i stałej temperatury poprzez użycie klimatyzacji. Serwerownia wyposażona jest w urządzenia podtrzymujące zasilanie w przypadku awarii. Ponadto stacje robocze wyposażone są w oprogramowanie antywirusowe i zabezpieczające system. Serwerownia oraz pomieszczenia biur są w sieci alarmowej, która jest pod ciągłym monitoringiem firmy ochroniarskiej. Lista osób uprawnionych do dostępu do poszczególnych pomieszczeń została określona w zarządzeniu Nr 53/2018 Wójta Gminy Stolno z dnia 23 maja 2018 r. w sprawie

[6] Dz. U. z 2018 r. poz. 1330, ze zm.
[7] Dz. U. Nr 10 poz. 68.

kontroli nadzoru nad ruchem osobowym w Urzędzie Gminy Stolno.
Urząd posiada podpisaną umowę z firmą informatyczną na bieżący nadzór informatyczny.
Ponadto na styku sieci urzędowej i Internetu został zastosowany programowy UTM (Endian).
Regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji oraz urządzeń mobilnych znajdują się w Polityce bezpieczeństwa informacji oraz Polityce ochrony danych.

Elementem zabezpieczeń techniczno-organizacyjnych dostępu do informacji jest również przyjęty sposób utylizacji sprzętu informatycznego i nośników danych. Zgodnie ze złożonymi wyjaśnieniami w kontrolowanym okresie sprzęt informatyczny nie był utylizowany. Natomiast jak wyjaśniono, w przypadku konieczności utylizacji bezużyteczny/uszkodzony sprzęt informatyczny jest pozbawiany wszelkich nośników danych, które podlegają fizycznemu zniszczeniu. Sprzęt bez nośników danych jest oddawany do PSZOK (punkt selektywnej zbiórki odpadów komunalnych). Kwestie te są uregulowane w Polityce bezpieczeństwa informacji oraz w Polityce ochrony danych w Urzędzie Gminy Stolno.

Jeśli chodzi o rozwiązania jakie funkcjonują w jednostce w zakresie mechanizmów kryptograficznych, np. dla transmisji do urządzeń mobilnych, poczty elektronicznej, a także podpisów kwalifikowanych do autoryzacji dokumentów to wskazać należy, że dostęp do systemów odbywa się za pomocą loginu i hasła potwierdzającego tożsamość danego użytkownika (w przypadku systemu ePUAP) lub za pomocą kart kryptograficznych (do systemu Źródło) wydanych przez uprawnione do tego organy. Ponadto ci pracownicy, którym posiadanie podpisu kwalifikowanego jest niezbędne w celu wykonywania swoich obowiązków (m.in. do autoryzacji dokumentów) posiadają karty kryptograficzne z podpisami kwalifikowanymi.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych.
Do kwestii zabezpieczeń techniczno-organizacyjnych systemów informatycznych odnosi się § 20 ust. 2 pkt 12 rozporządzenia KRI. Z kolei § 21 rozporządzenia KRI, wymaga obligatoryjnego odnotowywania działań użytkowników lub obiektów systemowych. Zgodnie z ust. 4 wspomnianego przepisu informacje w dziennikach systemów powinny być przechowywane od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata. Loga systemowe w przypadku BIP są przechowywane zgodnie z przepisami. W zakresie regulacji wewnętrznych do tych kwestii odnosi się Instrukcja zarządzania systemem informatycznym.

Stosowane systemy podlegają bieżącej aktualizacji, dotyczy to również oprogramowania antywirusowego. Ponadto użytkowane jest oprogramowanie zabezpieczające ruch sieciowy.
W celu minimalizowania ryzyka utraty informacji w wyniku awarii oraz w celu ochrony przed błędami, utratą i nieuprawnioną modyfikacją zastosowano system kopii zapasowych. Stosuje się autoryzowany dostęp do systemów (loginy i hasła, karty kryptograficzne). Zastosowano urządzenia podtrzymujące zasilanie w przypadku awarii. Stacje robocze wyposażone są w oprogramowanie antywirusowe i zabezpieczające system. Dostęp do serwerowni posiada zamknięta grupa osób, a wydawanie i zdawanie kluczy odbywa się w sposób umożliwiający rozliczalność.

2.14. Rozliczalność działań w systemach informatycznych.
Ten obszar został uregulowany w § 21 ust. 2-4 rozporządzenia KRI.
Regulacje wewnętrzne znajdują się w Instrukcji zarządzania systemem informatycznym.
Podgląd logów systemowych umożliwia zainstalowane oprogramowanie do zarządzania

siecią Axence nVision. Wspomaga ono kompleksową kontrolę dzienników z poziomu komputera administratora bez konieczności bezpośredniej fizycznej ingerencji na innych stanowiskach komputerowych. Natomiast w systemie BIP logi działalności użytkowników dostępne są z poziomu aplikacji po zalogowaniu na konto administracyjne. Logi przechowywane są w systemie ciągłym.

3. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych.
Strona Biuletynu Informacji Publicznej Urzędu Gminy Stolno umożliwia przełączanie na wersję kontrastową oraz skalowalność czcionki. Stronę www.bip.stolno.com.pl poddano walidacji pod kątem zgodności z WCAG 2.0. Została ona zweryfikowana jako zgodna na poziomie AA, co odpowiada wymaganiom określonym w § 19 rozporządzenia KRI.

Wskazuje się następujący zakres stwierdzonych uchybień:
- Polityka bezpieczeństwa informacji w Urzędzie Gminy Stolno ogranicza się w swoich regulacjach do kwestii bezpieczeństwa przetwarzania danych osobowych, a tylko pośrednio odnosi do bezpieczeństwa przetwarzania wszelkich innych informacji jakimi dysponuje podmiot kontrolowany. Ta sama uwaga dotyczy Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz Polityki ochrony danych w Urzędzie Gminy Stolno;
- tematyka przeprowadzanych szkoleń nie wyczerpuje zakresu wskazanego w § 20 ust. 2 pkt 6 rozporządzenia KRI;
- brak jest w umowie nr 03/17 z 2 stycznia 2017 r. *zobowiązania wykonawcy do zachowania w tajemnicy/nieudostępniania wszelkich informacji jakie pozyska w związku z realizacją umowy;*
- brak jest dokumentacji potwierdzającej wykonywanie, przechowywanie i testowanie kopii zapasowych;
- brak jest regulacji wewnętrznych opisujących proces monitorowania systemów teleinformatycznych i środowiska ich pracy pod kątem wydajności i pojemności w celu zapobieżenia ewentualnym problemom z tym związanym.

Wskazuje się następujący zakres stwierdzonych nieprawidłowości:
- w podmiocie kontrolowanym nie istnieją wewnętrzne procedury dotyczące obsługi usług elektronicznych oraz monitoringu dotyczącego dostarczania ich na zadeklarowanym poziomie.
Stanowi to naruszenie § 15 ust. 2 rozporządzenia KRI, w którym jest mowa o tym, że zarządzanie usługami realizowanymi przez systemy teleinformatyczne odbywa się w oparciu o udokumentowane procedury;
- nie stworzono sformalizowanych procedur w zakresie projektowania systemów teleinformatycznych dotyczących architektury systemu, sposobu licencjonowania i wykorzystania praw autorskich, zgodności z obowiązującym prawem (m.in. z ustawą o informatyzacji), sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, zastosowania rozwiązań funkcjonalnych odpowiednich dla osiągniecia założonych celów, prezentacji treści dla osób niepełnosprawnych, wydajności, poziomu niezawodności, w tym parametrów SLA na usługi serwisowe, mechanizmów kontroli i audytu. Narusza to § 15 rozporządzenia KRI;
- brak jest regulacji wewnętrznych opisujących wymagania w zakresie wdrażania systemów teleinformatycznych, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji a także warunków i kryteriów odbioru oraz regulacji wewnętrznych opisujących sposób przeprowadzania zmian

w systemach teleinformatycznych (w trakcie ich eksploatacji), w tym opisu: zgłaszania zmiany, analizy zmiany pod kątem wykonalności, kosztów, ryzyk, a także określenia sposobu wykonania i odbioru zmiany. Narusza to § 15 rozporządzenia KRI.

Ponadto wskazuje się następujące przyczyny i skutki stwierdzonych nieprawidłowości. Przyczyną stwierdzonych nieprawidłowości jest nieprzestrzeganie wskazanych przepisów rozporządzenia KRI. Skutkiem powyższego jest obniżenie możliwości zapewnienia bezpieczeństwa przetwarzanych informacji.

Za stwierdzone nieprawidłowości odpowiedzialność ponosi pracownik zatrudniony na stanowisku ds. administrowania siecią informatyczną, zamówień publicznych i pozyskiwania funduszy unijnych oraz z tytułu nadzoru Wójt Gminy Stolno.

Kontrolę wpisano do książki kontroli pod nr 2/2018.

Do Projektu wystąpienia pokontrolnego z dnia 14 września 2018 r. nie zostały zgłoszone zastrzeżenia.

W Projekcie wystąpienia pokontrolnego nie dokonano sprostowań, skreśleń ani uzupełnień.

W związku z powyższymi ocenami, uwagami i wnioskami zalecam Panu podjęcie następujących działań w celu wyeliminowania stwierdzonych w wyniku kontroli nieprawidłowości lub usprawnienia funkcjonowania działalności jednostki kontrolowanej:
- należy opracować wewnętrzne procedury dotyczące obsługi usług elektronicznych oraz monitoringu odnoszącego się do dostarczania ich na zadeklarowanym poziomie;
- należy opracować procedury w zakresie projektowania systemów teleinformatycznych dotyczące architektury systemu, sposobu licencjonowania i wykorzystania praw autorskich, zgodności z obowiązującym prawem (m.in. z ustawą o informatyzacji), sposobu i poziomu zabezpieczeń, zastosowania norm i standardów przemysłowych, zastosowania rozwiązań funkcjonalnych odpowiednich dla osiągniecia założonych celów, prezentacji treści dla osób niepełnosprawnych, wydajności, poziomu niezawodności, w tym parametrów SLA na usługi serwisowe, mechanizmów kontroli i audytu;
- należy opracować regulacje wewnętrzne opisujące wymagania w zakresie wdrażania systemów teleinformatycznych, wymagań sprzętowych i środowiskowych dla systemu, sposobu i zakresu testów odbiorowych oraz rodzaju i zakresu dokumentacji a także warunków i kryteriów odbioru oraz regulacji wewnętrznych opisujących sposób przeprowadzania zmian w systemach teleinformatycznych (w trakcie ich eksploatacji), w tym opisu: zgłaszania zmiany, analizy zmiany pod kątem wykonalności, kosztów, ryzyk, a także określenia sposobu wykonania i odbioru zmiany.

Wystąpienie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach, z których jeden egzemplarz otrzymuje kierownik jednostki kontrolowanej, a drugi egzemplarz pozostaje w aktach kontroli.

Oczekuję od Pana w terminie 30 dni od daty otrzymania niniejszego wystąpienia, informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

Wojewoda
Kujawsko-Pomorski