WOJEWODA MAZOWIECKI

Warszawa, 22 marca 2024 r.

WK-I.431.2.1.2023

Pan
Krzysztof Wolski
Starosta Kozienicki

Starostwo Powiatowe
w Kozienicach
ul. Jana Kochanowskiego 28
26-900 Kozienice

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 28 ust. 1 pkt 2 ustawy o wojewodzie i administracji rządowej w województwie[1], art. 6 ust. 4 pkt 3 ustawy o kontroli w administracji rządowej[2] oraz art. 25 ust. 1 pkt 3 lit. a ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[3], kontrolerzy: Anna Doroszewska i Kamil Karkułowski – starsi inspektorzy wojewódzcy, Łukasz Plaskot – kierownik Oddziału Serwisu Informatycznego w Biurze Informatyki oraz Mariusz Zmuda – specjalista w Oddziale Serwisu Informatycznego w Biurze Informatyki Mazowieckiego Urzędu Wojewódzkiego w Warszawie, przeprowadzili w dniach od 6 grudnia 2023 r. do 5 stycznia 2024 r. kontrolę problemową w Starostwie Powiatowym w Kozienicach, z siedzibą w Kozienicach przy ul. Jana Kochanowskiego 28 (dalej Starostwo).

Przedmiot kontroli obejmował działanie systemów teleinformatycznych używanych do realizacji zadań publicznych albo realizacji obowiązków wynikających z art. 13 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne pod względem zgodności z minimalnymi wymaganiami dla systemów teleinformatycznych

1 Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. 2023 r. poz. 190).
2 Ustawa z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224).
3 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307).

lub minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej[4] – w okresie od 1 stycznia 2023 r. do 22 listopada 2023 r.

Nawiązując do projektu wystąpienia pokontrolnego z 7 marca 2024 r., do którego nie wniesiono zastrzeżeń, przekazuję Panu Staroście wystąpienie pokontrolne.

Ocenie poddano trzy główne obszary kontroli, tj. wymianę informacji w postaci elektronicznej, w tym współpracę z innymi systemami informatycznymi oraz wspomaganie usług drogą elektroniczną, zarządzanie bezpieczeństwem informacji w systemach teleinformatycznych oraz zapewnienie dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych.

W Starostwie prowadzono rejestry publiczne, o których mowa w art. 14 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. W prowadzonych rejestrach publicznych wyróżniono typy obiektów oraz ustalono strukturę ich identyfikatorów, zgodnie z wymogami § 10 ust. 1, 2 i 3 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[5] (dalej rozporządzenie w sprawie KRI).

Kontroli poddano system teleinformatyczny *XXX* używany w Starostwie do realizacji zadań publicznych.

I. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami (rejestrami) teleinformatycznymi oraz wspomaganie usług drogą elektroniczną.

Starostwo udostępnia elektroniczną skrzynkę podawczą (dalej ESP) umożliwiającą doręczanie pism w formie dokumentów elektronicznych.

Na stronie internetowej Starostwa w zakładce *Formularze do pobrania* wyświetla się katalog wzorów wniosków pogrupowanych według komórek organizacyjnych odpowiedzialnych za realizację danego zadania, które można pobrać.

---

[4] Zgodnie z art. 25 ust. 3 przedmiotowej ustawy kontrola dotyczyła wyłącznie systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej.

[5] Rozporządzenie 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 (Dz. U. z 2017 r. poz. 2247).

Ustalono, że Starostwo w okresie objętym kontrolą nie przekazywało wzorów dokumentów elektronicznych do Centralnego Repozytorium Wzorów Dokumentów Elektronicznych, jak również nie korzystało z zasobów ww. repozytorium.

Starostwo stosuje w prowadzonych rejestrach odwołania do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań, zgodnie z § 5 ust. 3 pkt 3 rozporządzenia w sprawie KRI oraz wyposaża posiadane systemy teleinformatyczne w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanawianych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną UE, zgodnie z § 16 ust. 1 rozporządzenia w sprawie KRI oraz formatach danych określonych w załączniku nr 2 i 3 rozporządzenia w sprawie KRI.

Ustalono, że w Starostwie obowiązuje jako podstawowy, tradycyjny system obiegu dokumentów, a funkcjonujący system Elektronicznego Zarządzania Dokumentacją (dalej EZD) pełni funkcje wspomagające wykonywanie czynności kancelaryjnych w systemie tradycyjnym. System EZD jako narzędzie wspomagające podstawowy system zapewnia zintegrowaną obsługę korespondencji przychodzącej i wychodzącej poprzez rejestrację i zarządzanie obiegiem korespondencji oraz zakładanie i prowadzenie spraw oraz rejestrów[6].

W wyniku kontroli stwierdzono następujące nieprawidłowość polegającą na braku udokumentowanych procedur dotyczących dostarczania usług realizowanych przez systemy teleinformatyczne na deklarowanym poziomie dostępności, co jest niezgodne z § 15 ust. 2 rozporządzenia w sprawie KRI, zgodnie z którym: *„Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury”*.

Ponadto stwierdzono, że stronie Biuletynu Informacji Publicznej (dalej BIP) Starostwa nie zamieszczono informacji określonych w § 3 ust. 2-6 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępnia formularzy, wzorów i kopii dokumentów elektronicznych, zgodnie z którym: *„Podmioty publiczne informują na swoich stronach podmiotowych (...), o: 2) maksymalnym rozmiarze dokumentu elektronicznego*

[6] Powyższe uregulowane zostało Zarządzeniem nr 30/2022 Starosty Powiatu Kozienickiego z dnia 10 sierpnia 2015 r. w sprawie zmiany Zarządzenia Nr 19/2015 Starosty Powiatu Kozienickiego z dnia 10 sierpnia 2015 r. w sprawie wykonywania czynności kancelaryjnych w Starostwie Powiatowym w Kozienicach.

wraz z załącznikami, wyrażonym w megabajtach, możliwym do doręczenia za pomocą elektronicznej skrzynki podawczej, nie mniejszym niż 5 megabajtów; 3) zakresach użytkowych dokumentów elektronicznych (...); 4) rodzajach informatycznych nośników danych, na których może zostać im doręczony dokument elektroniczny; 5) rodzajach informatycznych nośników danych, na których może zostać zapisane urzędowe poświadczenie odbioru; 6) innych wymagań określonych przepisami prawa dotyczących doręczania dokumentów elektronicznych". W wyniku kontroli ustalono również, że na stronie BIP Starostwa po kliknięciu w zakładkę *Załatwianie spraw* następuje przekierowanie na stronę internetową, która w okresie poddanym kontroli nie zawierała żadnych wymaganych informacji[7].

Przedstawiając powyższe informuję, że realizację zadań dotyczących wymiany informacji w postaci elektronicznej, w tym współpracy z innymi systemami (rejestrami) teleinformatycznymi oraz wspomagania usług drogą elektroniczną ocenia się **pozytywnie pomimo stwierdzonych nieprawidłowości.**

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych.

W okresie objętym kontrolą w Starostwie obowiązywała Polityka Bezpieczeństwa Starostwa Powiatowego w Kozienicach (dalej: Polityka Bezpieczeństwa)[8] związana z problematyką przetwarzania i ochroną danych osobowych.

Obowiązujące w okresie kontrolowanym dokumenty opisują sposoby nadawania, modyfikacji i odbierania uprawnień użytkownikom, określają sposoby pracy w systemach informatycznych Starostwa, procedury zarządzania, a także czynności mające wpływ na zapewnienie bezpieczeństwa oraz zarządzania ryzykiem przetwarzania danych osobowych w systemach informatycznych.

Pracownicy wykonujący zadania w systemach teleinformatycznych uczestniczyli w procesie przetwarzania informacji w stopniu adekwatnym do przypisanych obowiązków, zgodnie z § 20 ust. 2 pkt 4 rozporządzenia w sprawie KRI. W trakcie trwania czynności kontrolnych analizie poddano historię nadawania i odbierania uprawnień do systemu *XXX* funkcjonującego w Starostwie dla 6 pracowników Wydziału XXX Starostwa, z okresu objętego kontrolą, tj.: dla dwóch nowozatrudnionych (nadanie uprawnień) oraz 4 użytkowników, którym

---

[7] XXX
[8] XXX

uprawnienia zostały odebrane, stwierdzając adekwatność poziomu uprawnień do pracy w systemach teleinformatycznych do zakresu czynności i realizowanych zadań.

Ustanowiono zasady gwarantujące bezpieczną pracę przy przetwarzaniu danych osobowych z wykorzystaniem urządzeń przenośnych i pracy na odległość, czym częściowo spełniono wymogi zawarte w § 20 ust. 2 pkt 8 powyższego rozporządzenia[9].

Stosownie do zapisów § 20 ust. 2 pkt 13 rozporządzenia w sprawie KRI, w Starostwie obowiązywały zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa danych osobowych uregulowane w obowiązujących ww. Polityce Bezpieczeństwa, natomiast z wyjaśnień uzyskanych podczas kontroli wynika, że w okresie objętym kontrolą zgłoszone incydenty nie podlegałyby zgłoszeniu w sposób określony w § 20 ust. 2 pkt 13 powyższego rozporządzenia.

W Starostwie obowiązywała procedura odnosząca się do tworzenia, przechowywania i testowania kopii zapasowych obowiązująca w okresie kontrolowanym[10], czym spełniono wymogi określone § 20 ust. 2 pkt 12 lit. b powyższego rozporządzenia.

W okresie objętym kontrolą nie wystąpiły przypadki projektowania i wdrażania systemów teleinformatycznych, wobec czego spełnienie warunków określonych w § 15 ust. 1 rozporządzenia w sprawie KRI nie było przedmiotem kontroli.

Zgodnie z wymogiem określonym w § 20 ust. 2 pkt 14 powyższego rozporządzenia, w okresie kontrolowanym w Starostwie przeprowadzono audyt w zakresie bezpieczeństwa informacji[11].

Regulacje wewnętrzne, w których ustalono zasady postępowania z informacjami w jednostce, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji w tym urządzeń oraz zasady dotyczące zapewnienia ochrony przetwarzanych informacji zostały zawarte w Polityce Bezpieczeństwa[12].

W toku kontroli ustalono, że zgodnie z zapisami § 20 ust. 2 pkt 7, 9, 11 i 12 rozporządzenia w sprawie KRI, Starostwo zapewnia ochronę przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także stosuje zabezpieczanie informacji w sposób uniemożliwiający osobom nieuprawnionym jej ujawnienie, modyfikację, usunięcie lub zniszczenie, poprzez:

- zapewnienie zewnętrznej i wewnętrznej ochrony fizycznej obiektów,

---

9 XXX.
10 XXX.
11 XXX
12 XXX.

- ustalenie zasad pobierania i zdawania kluczy do poszczególnych pomieszczeń Starostwa,
- ustanowienie regulacji wewnętrznych określających zasady postępowania z danymi osobowymi w jednostce, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń oraz zasad zapewniających odpowiedni poziom bezpieczeństwa systemów teleinformatycznych, a także zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych i pracy na odległość,
- zabezpieczenie serwerów i stacji roboczych aktualnym oprogramowaniem antywirusowym, automatycznie aktualizującym sygnatury wirusów,
- wykorzystywanie urządzeń brzegowych typu firewall,
- wyposażenie serwerów i urządzeń sieciowych w zasilanie awaryjne zabezpieczające system przed przepięciami i chwilowymi zanikami napięcia,
- ustanowienie regulacji wewnętrznych dotyczących tworzenia kopii zapasowych.

W wyniku kontroli stwierdzono następujące nieprawidłowości:

1. W okresie objętym kontrolą w Starostwie Powiatowym w Kozienicach nie funkcjonował System Zarządzania Bezpieczeństwem Informacji, o którym mowa w § 20 ust. 1 rozporządzenia w sprawie KRI. Obowiązująca w Starostwie Polityka Bezpieczeństwa reguluje wyłącznie zagadnienia związane z bezpieczeństwem danych osobowych[13]. Należy podkreślić, że dane osobowe stanowią jedynie część informacji przetwarzanych w Starostwie, natomiast zgodnie z § 20 ust. 1 rozporządzenia w sprawie KRI *„Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność”*.
2. Nie aktualizowano dokumentów dotyczących Polityki Bezpieczeństwa w zakresie zmieniającego się otoczenia[14], pomimo obowiązku wynikającego z § 20 ust. 2 pkt 1 rozporządzenia w sprawie KRI, zgodnie z którym: *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań (...) zapewnienia aktualizacji regulacji*

[13] XXX.
[14] Zgodnie z pisemnym wyjaśnieniem Pana Krzysztofa Wolskiego – Starosty Kozienickiego, XXX.

wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia (...)”. Przekazana do kontroli dokumentacja z obszaru bezpieczeństwa danych osobowych w Starostwie została wprowadzona w roku 2018 i w późniejszym okresie nie była aktualizowana.

3. W okresie objętym kontrolą nie przeprowadzano okresowej analizy ryzyka utraty integralności, dostępności lub poufności informacji[15], pomimo obowiązku wynikającego z § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI, zgodnie z którym: *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań (...) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy (...)”*.
4. Nie zapewniono aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej bazę konfiguracji CMDB[16], czym naruszono § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI, zgodnie z którym: *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań (...) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację (...)”*[17].
5. Nie zapewniono osobom zaangażowanym w proces przetwarzania informacji, szkoleń ze szczególnym uwzględnieniem zagadnień takich jak zagrożenia bezpieczeństwa wszystkich przetwarzanych informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna czy stosowanie środków zapewniających bezpieczeństwo informacji, czym naruszono wymogi § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI, zgodnie z którym: *„Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań (...) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:*

   a) zagrożenia bezpieczeństwa informacji,

   b) skutki naruszeń zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

---

[15] XXX.
[16] Configuration Management Database.
[17] Zgodnie z pisemnym wyjaśnieniem Pana Krzysztofa Wolskiego – Starosty Kozienickiego, XXX.

c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich".

6. W umowach[18] zawartych pomiędzy Powiatem Kozienickim a podmiotami zewnętrznymi nie zawarto dodatkowo zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, tj. umów powierzenia przetwarzania danych osobowych. Należy podkreślić, że obowiązek zawierania umów powierzenia przetwarzania danych osobowych wynika wprost z § 11 pkt 2-5 Polityki Bezpieczeństwa[19].
7. Przechowywano informacje w dziennikach systemów (logi) przez okres krótszy niż 2 lata[20], czym naruszono postanowienia § 21 ust. 4 rozporządzenia KRI, zgodnie z którym: *„Informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata"*.
8. Nadawano, zmieniano i odbierano uprawnienia w systemie XXX oraz innych systemach informatycznych Starostwa niezgodnie z zapisami obowiązującej w okresie kontrolowanym Polityki Bezpieczeństwa[21], poprzez nieprowadzenie szczegółowej dokumentacji potwierdzającej kiedy nadano, zmieniono lub odebrano ww. uprawnienia[22]. Kontrolującym nie przedłożono wniosków o nadanie, modyfikację bądź odebranie uprawnień w systemach informatycznych Starostwa dla losowo wybranych pracowników Wydziału XXX Starostwa.

Ponadto w toku kontroli ustalono, że w serwerowni Starostwa znajdującej się w budynku urzędu brak jest czujnika środowiskowego, tj. czujnika zalania, a także monitoringu wizyjnego wewnątrz pomieszczenia serwerowni jak i przed tym pomieszczeniem[23].

Przedstawiając powyższe informuję, że realizację zadań w zakresie działania systemu zarządzania bezpieczeństwem informacji w systemach teleinformatycznych ocenia się **negatywnie.**

[18] XXX
[19] XXX
[20] XXX
[21] XXX
[22] XXX
[23] XXX

III. Zapewnienie dostępności informacji zawartych na stronach internetowych jednostki dla osób niepełnosprawnych.

Strona internetowa Starostwa działająca pod adresem: https://www.kozienicepowiat.pl/ oraz Biuletynu Informacji Publicznej Starostwa https://bipkozienicepowiat.pl/ poddano weryfikacji zgodności ze standardem WCAG 2.0 za pomocą walidatorów http://validator.w3.org oraz http://jigsaw.w3.org/css-validator/. Przeprowadzona przez kontrolujących w dniu 6 grudnia 2023 r. walidacja ww. stron internetowych Starostwa za pomocą ww. walidatorów wykazała, że dla:

- walidatora https://validator.w3.org/ stwierdzono:
  - dla strony internetowej: https://www.kozienicepowiat.pl/ – 11 błędów, 20 ostrzeżeń oraz 85 komunikatów informacyjnych,
  - dla strony internetowej: https://bipkozienicepowiat.pl/ – 153 błędy, 38 ostrzeżeń oraz 66 komunikatów informacyjnych,
- walidatora http://jigsaw.w3.org/css-validator stwierdzono:
  - dla strony internetowej: https://www.kozienicepowiat.pl/ – 14 błędów oraz 588 ostrzeżeń,
  - dla strony internetowej: https://bipkozienicepowiat.pl/ – 11 błędów oraz 57 ostrzeżeń.

Wskazane w wyniku weryfikacji ww. strony internetowych błędy oraz ostrzeżenia nie miały wpływu na prezentowane treści[24].

Po weryfikacji ww. stron internetowych stwierdzono spełnienie wymagań WCAG 2.0 określonych w załączniku nr 4 rozporządzenia w sprawie KRI. W wyniku kontroli stwierdzono, że dostępna strona internetowa i strona Biuletynu Informacji Publicznej Starostwa zawierają rozwiązania techniczne umożliwiające osobom niepełnosprawnym zapoznanie się z treścią informacji, czym spełniono wymogi określone w § 19 powyższego rozporządzenia.

Przedstawiając powyższe informuję, że realizację zadania w przedmiocie zapewnienia dostępności informacji zawartych na stronach internetowych urzędu dla osób niepełnosprawnych ocenia się **pozytywnie**.

Mając na uwadze powyższe ustalenia zobowiązuję Pana Starostę do podjęcia działań w celu wyeliminowania ustalonych nieprawidłowości, a w szczególności do:

[24] Zgodnie z pisemnym wyjaśnieniem Pana Krzysztofa Wolskiego – Starosty Kozienickiego, XXX

1. Udokumentowania procedur dotyczących dostarczania i zarzadzania usługami na deklarowanym poziomie dostępności, zgodnie z § 15 ust. 2 rozporządzenia w sprawie KRI.
2. Opracowania, zatwierdzenia oraz wdrożenia dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji w Starostwie, zgodnie z regulacjami zawartymi w § 20 ust. 1 rozporządzenia w sprawie KRI.
3. Aktualizowania dokumentów dotyczących Polityki Bezpieczeństwa w warunkach zmieniającego się otoczenia, zgodnie z obowiązkiem wynikającym z § 20 ust. 2 pkt 1 rozporządzenia w sprawie KRI.
4. Przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności i poufności informacji, zgodnie z obowiązkiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia w sprawie KRI.
5. Zapewnienia aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji, obejmującej bazę konfiguracji CMDB, zgodnie z wymogiem określonym w § 20 ust. 2 pkt 2 rozporządzenia w sprawie KRI.
6. Zapewnienia osobom zaangażowanym w proces przetwarzania informacji, szkoleń ze szczególnym uwzględnieniem zagadnień takich jak zagrożenia bezpieczeństwa wszystkich przetwarzanych informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna czy stosowanie środków zapewniających bezpieczeństwo informacji, zgodnie z wymogami określonymi w § 20 ust. 2 pkt 6 rozporządzenia w sprawie KRI.
7. Zawierania w umowach dotyczących powierzenia przetwarzania danych osobowych z podmiotami zewnętrznymi dodatkowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji, zgodnie z wymogami określonymi w § 20 ust. 2 pkt 10 rozporządzenia w sprawie KRI oraz z § 11 pkt 2-5 Polityki Bezpieczeństwa Starostwa.
8. Przechowywania informacji w dziennikach systemów (logów) przez okres wskazany w § 21 ust. 4 rozporządzenia w sprawie KRI.
9. Nadawania/odbierania/zmiany uprawnień do systemów teleinformatycznych, w tym również do systemu XXX – zgodnie z postanowieniami § 20 ust. 2 pkt 4 i 5 rozporządzenia w sprawie KRI oraz zgodnie z zapisami obowiązującej Polityki Bezpieczeństwa Starostwa, poprzez prowadzenie szczegółowej dokumentacji potwierdzającej kiedy nadano, zmieniono lub odebrano ww. uprawnienia.

Ponadto wskazuję na konieczność:

- zamieszczenia na stronie BIP informacji określonych w § 3 ust. 2-6 rozporządzenia w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępnia formularzy, wzorów i kopii dokumentów elektronicznych,
- rozważenia możliwości doposażenia serwerowni zlokalizowanej w budynku Starostwa w czujnik środowiskowy (tj. czujnik zalania), a także w monitoring wizyjny wewnątrz pomieszczenia serwerowni jak i przed tym pomieszczeniem.

Przedstawiając powyższe informuję, że zgodnie z art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze oraz zobowiązuję Pana Starostę na podstawie art. 49 ww. ustawy do przekazania, w terminie 14 dni od daty otrzymania niniejszego wystąpienia pokontrolnego, pisemnej informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków pokontrolnych lub przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości. Proszę o przekazanie powyższej informacji za pośrednictwem platformy ePUAP.

Z up. WOJEWODY MAZOWIECKIEGO

Artur Subda
Dyrektor Wydziału Kontroli

/podpisano kwalifikowanym
podpisem elektronicznym/