Urząd Gminy Masłów
ul. Spokojna 2
26 - 001 Masłów

Sprawozdanie

z zadania zapewniającego przeprowadzonego

w Urzędzie Gminy Masłów

Temat zadania zapewniającego:

„Bezpieczeństwo Informacji w Urzędzie Gminy Masłów"

Audytor wewnętrzny:

[redacted]

MF 2108/2006

Masłów 2019

Spis treści

1. Cel zadania zapewniającego.

Ocena spełniania wymogów bezpieczeństwa informacji określonych w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz.U.2017 poz. 570) i wydanym do niej rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn. Dz.U.2017 poz. 2247), nazywanym dalej Rozporządzeniem KRI, w ramach oceny wymogów bezpieczeństwa informacji.

Celem audytu jest również sprawdzenie zgodności przetwarzania danych osobowych z zasadami, określonymi w:

1. Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018 poz. 1000);
2. Rozporządzeniu Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) nazywane dalej Ogólnym rozporządzeniem o ochronie danych osobowych lub RODO.

2. Podmiotowy zakres zadania zapewniającego.

Urząd Gminy Masłów
ul. Spokojna 2
26 - 001 Masłów

3. Przedmiotowy zakres zadania zapewniającego.

Przedmiotowy zakres zadania zapewniającego obejmuje:

1. Sprawdzenie sposobów realizacji zadań w zakresie spełnienia minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej i minimalnych wymagań dla systemów teleinformatycznych w zakresie sposobu zapewnienia bezpieczeństwa przy wymianie informacji oraz zastosowania standardów technicznych zapewniających interoperacyjność i bezpieczną wymianę informacji określonych w Rozporządzeniu KRI.
2. Przegląd oraz weryfikacja dokumentacji i procedur regulujących przetwarzanie danych osobowych w Urzędzie Gminy Masłów pod względem zgodności z obowiązującymi przepisami prawa.
3. Sprawdzenie środków technicznych i organizacyjnych zastosowanych do ochrony informacji, w tym ochrony danych osobowych.

4. Termin przeprowadzenia zadania zapewniającego.

Zadanie w fazie przygotowania i przeprowadzenia czynności audytowych zostało przeprowadzone w okresie od 01.12.2018 r. do 20.01.2019 r., po tym terminie sporządzono sprawozdanie z audytu.

5. Narzędzia i techniki przeprowadzania zadania audytowego

Dla przeprowadzenia badania obszaru objętego audytem, podjęto działania i zastosowano następujące techniki:

1) Badanie audytowe zgodnie z przyjętą listą kontrolną.
2) Zebranie wyjaśnień i dodatkowych informacji od Informatyka - Pana [redacted] - poprzez wypełnienie dwóch list kontrolnych:
    - Lista zgodności z KRI, która stanowi załącznik nr 1 do niniejszego sprawozdania;
    - Lista pytań do audytu stanowiąca załącznik nr 2 do niniejszego sprawozdania.
3) Weryfikacja/przegląd dokumentacji regulującej bezpieczeństwa informacji w Urzędzie Gminy Masłów.
4) Weryfikacja/przegląd dokumentacji regulującej bezpieczeństwo danych osobowych Urzędzie Gminy Masłów w tym Polityki Ochrony Danych wprowadzonej zarządzeniem Wójta Gminy Masłów nr 83/2018 z dnia 18 czerwca 2018 r.
5) Przegląd wydawanych przez Administratora Danych upoważnień do przetwarzania danych osobowych oraz ewidencji osób upoważnionych do przetwarzania danych osobowych prowadzonej przez Informatyka.
6) Przegląd umowy na wykonywanie funkcji Inspektora Ochrony Danych zawartej z Panem Radosławem Szymaszkiem, prowadzącym własną działalność gospodarczą pod firmą „Centrum Bezpieczeństwa Informatycznego Radosław Szymaszek" z siedzibą w Krasnymstawie.
7) Przegląd Rejestru Czynności Przetwarzania Danych Osobowych.
8) Przegląd umów powierzenia przetwarzania danych osobowych zawieranych przez Gminę Masłów. Przegląd dotyczył następujących umów:
    a) Umowy nr S.142.287.2018 zawartej w dniu 14 listopada 2018 r. pomiędzy Gminą Masłów reprezentowaną przez Tomasza Lato – Wójta Gminy Masłów a Panią [redacted] Rzeczoznawcą majątkowym;

b) Umowy o wzajemnym powierzeniu przetwarzania danych osobowych zawartej w dniu 07.08.2018 r. pomiędzy Skarbem Państwa – Krajowym Biurem Wyborczym z siedzibą w Warszawie reprezentowanym przez Adama Michalika, Dyrektora Delegatury Krajowego Biura Wyborczego w Kielcach a Gminą Masłów z siedzibą w Masłowie reprezentowaną przez Tomasza Lato – Wójta Gminy Masłów;

c) Umowy nr RGKIOŚ.142.182.2018.EN zawartej w dniu 20 lipca 2018 r. pomiędzy Gminą Masłów z siedzibą w Masłowie reprezentowaną przez Zastępcę Wójta Panią Monikę Dolezińską-Włodarczyk a Firmą Geo-System Sp. z o.o. z siedzibą w Warszawie, reprezentowaną przez Prezesa Zarządu - [redacted]

d) Umowy nr S.142.163.2018.EH zawartej w dniu 20 czerwca 2018 r. pomiędzy Gminą Masłów reprezentowaną przez Tomasza Lato – Wójta Gminy Masłów a Kancelarią Notarialną Violetta Zapała Notariusze spółka cywilna, reprezentowaną przez Notariusz Wiolettę Zapała;

e) Umowy nr 17/153/JU zawartej w dniu 22.12.2017 r. pomiędzy Gminą Masłów reprezentowaną przez Tomasza Lato – Wójta Gminy Masłów a ZETO SOFTWARE Spółka z ograniczoną odpowiedzialnością reprezentowaną przez Prezesa Zarządu – Panią [redacted]

f) Umowy zawartej w dniu 27 marca 2018r. w Masłowie pomiędzy Gminą Masłów reprezentowaną przez Tomasza Lato – Wójta Gminy Masłów a Asseco Data System S.A. z siedzibą w Gdyni reprezentowaną przez Jarosława Jastrzębskiego – Wiceprezesa Zarządu oraz [redacted] Wiceprezesa Zarządu;

g) Umowy nr RGKIOŚ.142.112.2018.EH zawartej w dniu 11.05.2018 r. pomiędzy Gminą Masłów reprezentowaną przez Tomasza Lato – Wójta Gminy Masłów a Kancelarią Prawną Jakóbik i Ziemba reprezentowaną przez adwokata [redacted]

h) Umowy nr S.142.149.2017.ZZ zawartej w dniu 23 czerwca 2017 r. pomiędzy Gminą Masłów reprezentowaną przez Tomasza Lato – Wójta Gminy Masłów a Sun Gallo s.c z siedzibą w Łodzi reprezentowaną przez Właściciela [redacted]

i) Umowy nr 1406/4388/SB/2018 zawartej w dniu 23 listopada 2018 roku pomiędzy Gminą Masłów reprezentowaną przez Tomasza Lato – Wójta Gminy Masłów a INTERmedi@ Ł.Czekała T. Frąckowiak Spółka Jawna reprezentowaną przez [redacted] - Dyrektor Zarządzający/Wspólnik.

6. Sposób klasyfikowania wyników dla poszczególnych kryteriów oceny ustaleń stanu faktycznego

Dla stwierdzonych w toku zadania audytowego ustaleń, przyjęto trzy poziomy istotności:

1) poziom I – wskaźnik ważności niski, ustalenia o umiarkowanym znaczeniu, ich charakter i rozmiar dla audytowanej działalności nie stanowi zagrożenia, wymaga jednak podjęcia działania przez Kierownika komórki audytowanej,

2) poziom II – wskaźnik ważności średni, ustalenie o istotnym znaczeniu dla działalności audytowanej, ich charakter i rozmiar wymaga podjęcia działań przez Kierownika komórki audytowanej oraz powiadomienia osób nadzorujących,

3) poziom III – wskaźnik ważności wysoki, ustalenia o najwyższym znaczeniu dla audytowanego obszaru działalności, wymagającego pilnego podjęcia działań przez Kierownika komórki audytowanej oraz powiadomienia osób nadzorujących, np.:

   - zagrożenie bezpieczeństwa ludzi,
   - czyny niezgodne z prawem,
   - utrata znacznego majątku,
   - brak osiągnięcia kluczowych celów,
   - negatywny wpływ na wizerunek jednostki,
   - nierzetelna sprawozdawczość wewnętrzna lub zewnętrzna.

7. Kryteria oceny ustaleń stanu faktycznego oraz ustalenia stanu faktycznego

7.1. System Zarządzania Bezpieczeństwem Informacji

Kryteria oceny stanu faktycznego:

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn. Dz.U.2017 poz. 570);

2. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn. Dz.U.2017 poz. 2247), nazywanym dalej KRI lub rozporządzeniem KRI.

Ustalenia stanu faktycznego:

Urząd Gminy w Masłowie jest podmiotem realizującym zadnia publiczne, zatem Jednostka zgodnie z §20 ust. 1 rozporządzenia KRI zobowiązana jest do opracowania i ustanowienia, wdrożenia i eksploatacji, monitorowania i przeglądania oraz utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji (dalej SZBI). System ten powinien zapewniać poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Ustalenia audytora w tym zakresie są następujące:

1. Po zapoznaniu się z Polityką Ochrony Danych obowiązująca w Urzędzie Gminy Masłów audytor stwierdził iż:
   - celem jej wdrożenia było zdefiniowanie ogólnych wymagań i zasad ochrony, które będą fundamentem dla wszystkich dokumentów związanych z ochroną danych osobowych;
   - Polityka została przygotowana w oparciu o podstawy prawne dotyczące przetwarzania jedynie danych osobowych tj. rozporządzenie RODO i ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.

   Wynika z tego, iż dokument ten reguluje jedynie kwestie związane przetwarzaniem danych osobowych. W Urzędzie Gminy w Masłowie nie opracowano i nie wdrożono kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji, nie wdrożono również Polityki Bezpieczeństwa Informacji, która jest bardzo istotnym elementem tego systemu. Z informacji uzyskanych z listy zgodności wypełnionej przez Pana [redacted] wynika, iż do 18 czerwca 2018 roku w Jednostce była wdrożona Polityka Bezpieczeństwa Informacji lecz w chwili obecnej obowiązuje jedynie Polityka Ochrony Danych, która nie reguluje przetwarzania wszystkich kategorii informacji.

   Informatyk Pan [redacted] udzielił dodatkowych wyjaśnień, z których wynika, że wdrożona w Urzędzie Gminy Polityka Ochrony Danych jest przygotowana w oparciu o rozporządzenie w sprawie Krajowych Ram Interoperacyjności, nie jest to jednak dokładnie wskazany w §20 system zarządzania bezpieczeństwem informacji. W opinii audytora Polityka Ochrony Danych funkcjonująca w Urzędzie zawiera wprawdzie kilka wymaganych w §20 rozporządzenia KRI elementów, lecz nie spełnia w pełni tych wymagań.
2. W związku z brakiem całościowych regulacji dotyczących Systemu Zarządzania Bezpieczeństwem Informacji w Jednostce nie są realizowane (lub są realizowane jedynie w odniesieniu do danych osobowych) następujące wymagania określone w rozporządzeniu KRI:

a) Nie zapewniono aktualizacji regulacji wewnętrznych dotyczących bezpieczeństwa informacji w zakresie dotyczącym zmieniającego się otoczenia (zgodnie z §20 ust. 2 pkt. 1 rozporządzenia KRI);

b) Nie są przeprowadzane okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji (zgodnie z §20 ust. 2 pkt. 3 rozporządzenia KRI). Z informacji uzyskanych od Pana [redacted] wynika, iż Jednostka jest w trakcie wykonywania analizy ryzyka. Z przedstawionego audytorowi dokumentu „Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych w Urzędzie Gminy w Masłowie wynika, iż wykonywana analiza ryzyka dotyczy wyłącznie operacji przetwarzania danych osobowych;

c) Nie przeprowadzono szkoleń osób zaangażowanych w proces przetwarzania informacji, (zgodnie z §20 ust. 2 pkt. 6 rozporządzenia KRI). Szkolenia, które były przeprowadzane dla pracowników Urzędu Gminy w Masłowie dotyczyły jedynie ochrony danych osobowych. Z wyjaśnień udzielonych przez Informatyka pana [redacted] wynika, iż szkolenia z tego zakresu były organizowane cyklicznie przez Centrum Bezpieczeństwa Informatycznego. Audytorowi zostały udostępnione skany certyfikatów wydanych pracownikom, którzy odbyli szkolenia. Po przeanalizowaniu tych certyfikatów audytor stwierdza, iż potwierdzają one jedynie odbycie jednego szkolenia, którego temat brzmi: „Bezpieczeństwo i ochrona informacji wg. wymogów ustawy o ochronie danych osobowych". Szkolenie odbyło się w dniu 18 maja 2017 r. Zakres szkolenia potwierdza, iż jego tematyka dotyczyła jedynie danych osobowych;

3. Mimo braku całościowych regulacji dotyczących SZBI, znaczna część wymagań określonych w KRI jest jednak realizowana w Urzędzie Gminy w Masłowie. Dzięki rozbudowanemu systemowi ochrony danych osobowych, który reguluje przetwarzanie i zabezpieczanie danych w wielu obszarach, spełnione są całościowo lub częściowo niektóre wymagania KRI.

   Są to między innymi:

   a.) Z informacji uzyskanych od Informatyka - Pana [redacted] wynika iż prowadzona jest aktualna inwentaryzacja sprzętu informatycznego. W ramach audytu cyklicznie wykonywanego przez Centrum Bezpieczeństwa Informatycznego przeprowadzana jest inwentaryzacja oprogramowania. Zatem spełnione są wymagania określone w §20 ust. 2 pkt. 2 rozporządzenia KRI;

   b.) Opracowano i wdrożono procedury dotyczące zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach informatycznych. Wprawdzie regulacje obowiązujące w Urzędzie Gminy w Masłowie dotyczą jedynie danych osobowych, ale ich wdrożenie zapewnia również bezpieczeństwo pozostałym informacjom przetwarzanym w systemie informatycznym

Jednostki. Częściowo spełniony jest zatem wymóg określony w §20 ust. 2 pkt. 12 rozporządzenia KRI;

c.) Wdrożono podstawowe zasady gwarantujące bezpieczną pracę na odległość oraz przy przetwarzaniu mobilnym. Z informacji uzyskanych od Pana [redacted] wynika, iż w Jednostce używane są systemy informatyczne wykorzystujące „pracę na odległość". Połączenia do serwerów Gminy z jednostek podległych zabezpieczane są poprzez stosowanie bezpiecznych, szyfrowanych połączeń IPcec VPN. Spełniony jest zatem wymóg określony w §20 ust. 2 pkt. 8 rozporządzenia KRI;

d.) Podejmowane są działania zapewniające, 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. Podejmowane są również działania mające na celu bezzwłoczną zmianę uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji. Polityka Ochrony Danych zawiera również zapisy obligujące Informatyka do przeprowadzenia okresowej kontroli uprawnień - co najmniej raz na kwartał. Informatyk przedstawił dokument potwierdzający wykonanie w dniu 17 grudnia 2018 r. ww. kontroli uprawnień;

Ponieważ opisy procedur dotyczących nadawania i cofania uprawnień oraz ich kontroli zawarte w Polityce Ochrony Danych dotyczą jedynie danych osobowych, wymóg określony w §20 ust. 2 pkt. 4 i 5 rozporządzenia KRI jest spełniony częściowo. W Jednostce brakuje również procedur opisujących sposób dokumentowania nadawania, modyfikowania i odbierania uprawnień pracownikom;

e.) Wdrożono zabezpieczenia, które chronią przetwarzane informacje przed kradzieżą, nieupoważnionym dostępem, uszkodzeniem lub zakłóceniami. Wprawdzie przyjęte i opisane procedury w tym zakresie dotyczą jedynie danych osobowych, jednak ich wdrożenie i zastosowanie zapewnia odpowiedni poziom bezpieczeństwa pozostałym informacjom przetwarzanym w systemie informatycznym Jednostki. Zatem można uznać, że spełnione są wymagania określone w §20 ust. 2 pkt. 7 rozporządzenia KRI;

f.) Z informacji uzyskanych od Informatyka wynika, iż w Urzędzie Gminy w Masłowie wdrożono również zabezpieczenia uniemożliwiające nieuprawnionej osobie ujawnienie, modyfikację, usunięcie lub zniszczenie informacji. Zatem spełnione są wymagania określone w §20 ust. 2 pkt. 9 rozporządzenia KRI;

g.) W umowach serwisowych zawartych przez Urząd Gminy w Masłowie ze stronami trzecimi znajdują się zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji. Dzięki tym działaniom Jednostka spełnia wymóg określony w §20 ust. 2 pkt. 10 rozporządzenia KRI;

h.) W Urzędzie Gminy w Masłowie opracowano i wdrożono procedury dotyczące zgłaszania i postępowania z incydentami. Regulacje te opisane są w załączniku nr 18 do Polityki Ochrony Danych. Procedury te dotyczą jedynie incydentów dotyczących danych osobowych, zatem tylko częściowo jest spełniony wymóg określony w §20 ust. 2 pkt. 13 rozporządzenia KRI;

i.) W Urzędzie Gminy w Masłowie zapewniono okresowy audyt dotyczący bezpieczeństwa informacji. W rozdziale 20 Polityki Ochrony Danych znajdują się zapisy zobowiązujące jednostkę do przeprowadzenia ww. audytu nie rzadziej niż raz na rok, które są zgodne z zapisami §20 ust. 2 pkt. 14 rozporządzenia KRI. Ponieważ nie przedstawiono audytorowi dokumentów potwierdzających wykonanie tego obowiązku w latach wcześniejszych, w opinii audytora wymóg ten jest spełniony jedynie częściowo;

j.) Z informacji uzyskanych od Informatyka wynika, iż w Urzędzie Gminy w Masłowie są zbierane i przechowywane w postaci elektronicznej zapisy w dziennikach systemów (logach) informacje zapewniające rozliczalność działań użytkowników i administratorów. Ponieważ nie wszystkie informacje wymagane rozporządzeniem KRI są zbierane oraz nie określono czasu ich przechowywania wymagania §21 rozporządzenia KRI są spełnione tylko częściowo.

Słabości/Ryzyka:

1. Opracowane i wdrożone w Urzędzie Gminy w Masłowie regulacje dotyczące zagadnień związanych z bezpieczeństwem informacji nie obejmują wszystkich kategorii informacji przetwarzanych w Jednostce, lecz dotyczą jedynie danych osobowych.
   Dnia 18 czerwca 2018 (zarządzenie Wójta Gminy Masłów NR 83/2018) została wprowadzona Polityka Ochrony Danych zastępująca obowiązującą wcześniej Politykę Bezpieczeństwa Informacji.
   Urząd Gminy w Masłowie - jako Jednostka realizująca zadania publiczne zobowiązana jest do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) – zgodnie z §20 rozporządzenia KRI. Polityka Bezpieczeństwa Informacji powinna być dokumentem, który reguluje przetwarzanie wszystkich kategorii informacji (nie tylko danych osobowych).
2. Z przeprowadzonej analizy dokumentacji oraz działań wykonywanych w Urzędzie Gminy w Masłowie wynika, iż w Jednostce nie wyznaczono osób odpowiedzialnych za przygotowanie, wdrożenie kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji. Wdrażane w Jednostce regulacje i procedury koncentrowały się głównie na zapewnieniu ochrony danych osobowych.
   Nie dostrzegano konieczności szerszego podejścia do ochrony wszystkich informacji

przetwarzanych w Jednostce. Ponieważ jednak opracowany i wdrożony system ochrony danych osobowych jest bardzo rozbudowany i równocześnie realizowane są kompleksowe działania zapewniające szeroko rozumiane bezpieczeństwo systemów informatycznych, wiele wymagań dotyczących bezpieczeństwa informacji określonych w rozporządzeniu KRI jest realizowane oraz spełniane całościowo lub częściowo. Niezależnie jednak od wykonywanych działań, w Jednostce brakuje dokumentacji i procedur określających bezpieczne sposoby przetwarzania informacji, które powinny dokumentować działania wymagane rozporządzeniem KRI.

3. W Jednostce nie zapewniono szkoleń z zakresu bezpieczeństwa informacji, dokumenty przekazane audytorowi potwierdzają jedynie szkolenia pracowników z zakresu ochrony danych osobowych.

Zalecenia:

1. Zgodnie z §20 rozporządzenia KRI należy opracować i ustanowić, wdrożyć i eksploatować, monitorować i przeglądać, utrzymywać i doskonalić System Zarządzania Bezpieczeństwem Informacji. System ten powinien zapewniać poufność, dostępność i integralność wszystkich informacji przetwarzanych w Urzędzie Gminy w Masłowie z uwzględnieniem takich atrybutów jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Niezbędnym elementem tego systemu powinna być Polityka Bezpieczeństwa Informacji, która będzie stanowić zbiór reguł, zasad i procedur stosowanych przez Urząd Gminy w Masłowie w celu osiągnięcia interoperacyjności oraz odpowiedniego poziomu bezpieczeństwa w odniesieniu do wszystkich przetwarzanych informacji (nie tylko danych osobowych). Ponieważ w Jednostce opracowano i wdrożono system ochrony danych osobowych, który reguluje wiele obszarów opisanych w rozporządzenia KRI można rozważyć dostosowanie tego systemu do ochrony nie tylko danych osobowych, ale również pozostałych informacji. W opinii audytora takie działanie jest zasadne i mniej pracochłonne niż tworzenie systemu zarządzania bezpieczeństwem informacji od podstaw. Należy rozważyć dostosowanie/zmianę dokumentów i procedur dotyczących przetwarzania danych osobowych w taki sposób, aby dotyczyły wszystkich informacji przetwarzanych w Jednostce (w tym danych osobowych). W przypadku obszarów, które nie są objęte procedurami stosowanymi w Jednostce, a są wymagane rozporządzeniem KRI, należy stworzyć i wdrożyć procedury, które będą regulowały brakujące obszary związane z bezpieczeństwem informacji. Zbiór wszystkich regulacji stworzy Politykę Ochrony Informacji, która powinna stanowić kluczowy element Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy w Masłowie.

2. Zgodnie z §20 ust. 2 pkt. 6 należy zapewnić szkolenia osób zaangażowanych w przetwarzanie informacji. Tematyka szkoleń powinna być dostosowana do wymagań stawianych przez rozporządzenie KRI, dotyczących przetwarzania wszystkich rodzajów informacji (nie tylko danych osobowych). Szkolenia pracowników należy dokumentować poprzez odnotowanie listy przeszkolonych pracowników, daty szkolenia oraz zakresu szkolenia.

7.2. Obszar Ochrony Danych Osobowych

Kryteria oceny ustaleń stanu faktycznego:

1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2018 poz. 1000) nazywana dalej UoDO;
2. Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) nazywane dalej Ogólnym rozporządzeniem o ochronie danych osobowych lub RODO).

Ustalenia stanu faktycznego:

1. W Urzędzie Gminy w Masłowie, Zarządzeniem Wójta Gminy Masłów nr 83/2018 z dnia 18 czerwca 2018 r., wprowadzono Politykę Ochrony Danych Osobowych. Dokument ten reguluje i określa zasady dotyczące przetwarzania danych osobowych w Urzędzie Gminy w Masłowie. Polityka Ochrony Danych Osobowych zawiera 22 strony, do Polityki dołączono 22 załączniki.
2. Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego art. 29 RODO.

   W Polityce Ochrony Danych Osobowych została opisana procedura nadawania upoważnień do przetwarzania danych osobowych, w procedurze tej określono wzór upoważnienia oraz wzór ewidencji osób upoważnionych. Po sprawdzeniu audytor stwierdził, iż Administrator Danych wydał stosowne upoważnienia do przetwarzania danych osobowych dla pracowników Jednostki mających dostęp do danych osobowych. Audytor po sprawdzeniu wydanych upoważnień nie stwierdził nieprawidłowości w tym zakresie.
3. Obowiązki określone w art. 30 RODO - Prowadzenie Rejestru Czynności Przetwarzania Danych Osobowych (dalej RCP) i Rejestru Wszystkich Kategorii Czynności Przetwarzania (dalej RWKCP) – art. 30 RODO.

W Urzędzie Gminy w Masłowie prowadzony jest Rejestr Czynności Przetwarzania.

Po sprawdzeniu ww. Rejestru audytor stwierdził, iż:

a) Rejestr pod względem formalnym jest prawidłowy, tzn. daje możliwość odnotowania wszystkich informacji wymaganych w art. 30 ust. 1 RODO;

b) Pole „kategorie odbiorców" (kolumna nr 6) jest wypełniony nieprawidłowo. Według definicji RODO: „odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania";

W rejestrze prowadzonym w Jednostce dla większości czynności w nim odnotowanych, w polu tym znajduje się informacja nd. W opinii audytora w polu tym należy zawrzeć informacje o wszystkich kategoriach odbiorców, którym Jednostka ujawnia dane, w ramach wykonywania danej czynności przetwarzania. Przykładem takiej czynności jest np. wypłata wynagrodzeń, w celu wykonania tej czynności Jednostka ujawnia dane osobowe pracowników, ZUS-owi, Urzędom Skarbowym, bankowi który obsługuje Jednostkę. Podobne nieprawidłowości znajdują się w innych kategoriach przetwarzania opisanych w rejestrze. W rejestrze nie odnotowano również informacji o ujawnianiu danych osobowych w związku z realizacją umów powierzenia przetwarzania, zawartych przez Jednostkę. Podmioty przetwarzające, którym Administrator powierza przetwarzanie danych, również są odbiorcami zgodnie z definicją z RODO.

c) Rejestr jest prowadzony w zbyt ogólnej formie, tzn. niektóre czynności przetwarzania wyszczególnione w rejestrze mają zbyt ogólny charakter. Zdaniem audytora w rejestrze nie odnotowano kilku czynności przetwarzania danych realizowanych przez Urząd (brakuje np. czynności związanych z obsługą wniosków o udostępnienie informacji publicznej).

W Urzędzie Gminy w Masłowie nie jest prowadzony Rejestr Wszystkich Kategorii Czynności Przetwarzania Danych Osobowych. Z informacji uzyskanych od Informatyka pana [redacted] wynika, iż Inspektor Ochrony Danych jest na etapie analizy obszarów przetwarzania danych w Urzędzie Gminy Masłów, pod kątem wprowadzenia rejestru kategorii czynności.

4. Obowiązki Administratora określone w art. 24 RODO.

   Po sprawdzeniu dokumentów, procedur oraz regulacji dotyczących przetwarzania danych osobowych w Urzędzie Gminy w Masłowie audytor stwierdza, iż Administrator Danych wypełnia obowiązki określone w art. 24 RODO w sposób prawidłowy. Uwzględniając zakres, kontekst, cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych, których dane osobowe są przetwarzane w Jednostce. Administrator wdrożył odpowiednie środki techniczne i organizacyjne zapewniające, że przetwarzanie odbywa się zgodnie z rozporządzeniem RODO. Administrator wdrożył również odpowiednie procedury, które dokumentują działania podejmowane w zakresie ochrony danych osobowych i jest w stanie wykazać zgodność przetwarzania danych osobowych z rozporządzeniem RODO. Cele te Administrator zrealizował poprzez wdrożenie Polityki Ochrony Danych wraz z załącznikami. Dokument ten reguluje przetwarzanie danych osobowych w Jednostce. Administrator zapoznał wszystkich pracowników z ww. regulacjami. W ogólnej klauzuli informacyjnej dotyczącej przetwarzania danych osobowych w Jednostce Administrator przekazuje osobom, których dane przetwarza informacje wymagane w art. 13 i 14 RODO. Klauzula ta jest dostępna na stronie internetowej Gminy pod adresem: https://www.maslow.pl/asp/pl_start.asp?typ=14&menu=233&strona=1.

5. Obowiązek Informacyjny art. 13 i art. 14 RODO

   W wyniku przeprowadzenia analizy dokumentów i regulacji obowiązujących w Urzędzie Gminy w Masłowie audytor stwierdza, iż w Jednostce opracowano procedury określające sposób realizacji obowiązku informacyjnego określonego w art. 13 i 14 RODO. Procedury te zostały opisane w rozdziale 7.1 Polityki Ochrony Danych. W Jednostce opracowano również „Wzór Klauzuli Informacyjnej", który stanowi załącznik nr 4 do Polityki Ochrony Danych. Na stronie internetowej Jednostki pod adresem https://www.maslow.pl/asp/pl_start.asp?typ=14&menu=233&strona=1 znajduje się klauzula zawierająca informacje na temat przetwarzania danych przez Urząd Gminy w Masłowie.

   Zdaniem audytora realizacja zapisów rozdziału 7.1 Polityki Ochrony Danych zapewnia prawidłowe wypełnienie obowiązków informacyjnych określonych w art. 13 i 14 RODO.

6. Prawa osób, których dane dotyczą art. 15-21 RODO.

   W opinii audytora regulacje dotyczące przetwarzania danych osobowych w Urzędzie Gminy w Masłowie prawidłowo opisują sposoby realizacji praw osób fizycznych, których dane są przetwarzane w Jednostce. W klauzulach informacyjnych osoby, których dane dotyczą są informowane o przysługujących im prawach i sposobach ich egzekwowania. Dzięki temu każda

osoba, której dane osobowe są przetwarzane w Urzędzie ma możliwość skorzystania ze swoich uprawnień określonych w RODO.

7. Wyznaczenie Inspektora Ochrony Danych Osobowych art. 37 RODO i rozdział 2 UoODO. Zgodnie z zapisami art. 37 ust. 1 RODO i rozdziałem 2 UoODO Urząd Gminy w Masłowie jest zobowiązany do wyznaczenia Inspektora Ochrony Danych. Obowiązek ten został zrealizowany w sposób prawidłowy. W dniu 25.09.2018 r. podpisano umowę z Panem [redacted] prowadzącym własną działalność pod firmą „Centrum Bezpieczeństwa Informatycznego Radosław Szymaszek", który od tego dnia pełni funkcję Inspektora Ochrony Danych Osobowych w Urzędzie Gminy w Masłowie.
   W umowie znajdują się zapisy, w których „Zleceniobiorca" oświadcza, iż posiada odpowiednią wiedzę, doświadczenie, niezbędne zaplecze prawne, sprzętowe materiałowe oraz personalne w zakresie pełnienia funkcji Inspektora Ochrony Danych.
   Zgodnie z wymogiem prawnym Inspektor Ochrony Danych został zgłoszony w dniu 10.08.2018 r. do rejestru prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych.
   Po przeanalizowaniu ww. umowy oraz zgłoszenia audytor stwierdza, że zawarte w umowie zapisy w prawidłowy sposób określają sposób pełnienia funkcji Inspektora Ochrony Danych Osobowych. Zgłoszenia dokonano również w prawidłowy sposób.

8. Zadania Inspektora Ochrony danych art. 39 RODO.

   Zadania Inspektora Ochrony Danych Osobowych zostały określone w umowie zawartej z Panem [redacted] prowadzącym własną działalność pod firmą „Centrum Bezpieczeństwa Informatycznego Radosław Szymaszek" oraz w rozdziale 6.2 Polityki Ochrony Danych obowiązującej w Jednostce. W opinii audytora ww. dokumenty w prawidłowy sposób określają zadania i obowiązki wykonywane przez Inspektora Ochrony Danych Osobowych i są zgodne z wymaganiami określonymi w art. 39 RODO.

9. Zgłoszenie i dokumentowanie naruszeń ochrony danych osobowych art.33 RODO.

   Zgodnie z zapisami art. 33. RODO Administrator ma obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków i podjętych działań zaradczych. W przypadku, gdy naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator ma obowiązek zgłosić takie naruszenie do Prezesa Urzędu Ochrony Danych Osobowych.

   W Urzędzie Gminy w Masłowie określono procedury identyfikacji i klasyfikacji naruszeń ochrony danych osobowych, ich dokumentowania, oceny oraz ewentualnego zgłaszania do Urzędu

Ochrony Danych Osobowych. Regulacje te są zawarte w rozdziale 17 Polityki Ochrony Danych oraz w załącznikach nr 18, 19 i 20 do ww. Polityki. Zapisy te określają sposoby postępowania w przypadku wystąpienia naruszenia ochrony danych osobowych w Jednostce oraz obowiązki poszczególnych pracowników w tym zakresie. W Jednostce wskazano również sposób rejestrowania naruszeń ochrony danych osobowych, w załączniku nr 19 do Polityki Ochrony Danych znajduje się wzór prowadzenia tego rejestru.

Po analizie procedur dotyczących postępowania w przypadku wystąpienia naruszeń w Urzędzie Gminy w Masłowie audytor nie stwierdził nieprawidłowości w tym zakresie.

10. Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych art.33 RODO.

    Zgodnie z zapisami Procedury zgłaszania naruszeń ochrony danych osobowych obowiązującej w Urzędzie Gminy w Masłowie, Administrator Danych bez zbędnej zwłoki zawiadamia osobę o naruszeniu danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

    W opinii audytora procedura dotycząca informowania osób, których dane dotyczą opisana w Polityce jest prawidłowa.

11. Powierzenie przetwarzania art. 28 RODO.

    W art. 28 RODO znajdują się regulacje przetwarzania danych osobowych w imieniu Administratora (powierzenia przetwarzania). Obligują one Administratora do korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych by przetwarzanie spełniało wymogi RODO i chroniło prawa i wolność osób, których dane dotyczą.

    Audytor dokonał analizy Polityki Ochrony Danych pod kątem regulacji dotyczących powierzania przetwarzania danych osobowych. Zapisy regulujące kwestie powierzenia przetwarzania danych określono w rozdziale 19 Polityki Ochrony Danych. Administrator przyjął również minimalne wymogi co do umowy powierzenia przetwarzania danych osobowych i opisał je we wzorze stanowiącym załącznik nr 16 do Polityki Ochrony Danych Osobowych. Po analizie ww. dokumentów oraz analizie umów powierzenia przetwarzania z podmiotami, którym administrator powierzył przetwarzanie danych we własnym imieniu, audytor stwierdził pewne nieprawidłowości w tym zakresie.

    Kilka umów powierzenia przetwarzania danych osobowych zawartych przez Jednostkę jest niezgodne z rozporządzeniem RODO oraz z regulacjami zawartymi w rozdziale 16 Polityki Ochrony Danych.

Umowa nr S.142.287.2018 zawarta w dniu 14 listopada 2018 r. pomiędzy Gminą Masłów reprezentowaną przez Tomasza Lato – Wójta Gminy Masłów a Panią [redacted] Rzeczoznawcą majątkowym, zawiera nieaktualną podstawę prawną (ustawę o ochronie danych osobowych, która już nie obowiązywała w dniu podpisywania umowy). W umowie tej nieprawidłowo określono Administratora i Podmiot Przetwarzający (użyto określeń Zleceniodawca i Zleceniobiorca). Umowa jest niezgodna ze wzorem Umowy Powierzenia Przetwarzania stanowiącym załącznik nr 16 do Polityki Ochrony Danych. Z ww. powodów umowa ta nie spełnia wymagań art. 28 RODO.

Podobne nieprawidłowości występują, również w innych umowach powierzenia przetwarzania zawieranych przez Urząd Gminy w Masłowie.

Słabości/Ryzyka:

1. Nieprawidłowości w prowadzeniu Rejestru Czynności Przetwarzania skutkują tym, iż obowiązki określone w art. 30 RODO nie są w pełni spełnione, naraża to Jednostkę na sankcje prawne przewidziane w rozdziale 11 Ustawy o Ochronie Danych Osobowych z dnia 10 maja 2018 r.
2. Brak Rejestru Wszystkich Kategorii Przetwarzania Danych Osobowych jest naruszeniem art. 30 ust. 2. Rozporządzenia RODO i naraża Jednostkę na sankcje prawne przewidziane w rozdziale 11 Ustawy o Ochronie Danych Osobowych z dnia 10 maja 2018 r. Prowadzona obecnie analiza, której celem jest określenie czy ww. rejestr jest w Jednostce potrzebny, jest działaniem prawidłowym, lecz spóźnionym. Analizy takiej należało dokonać w maju 2018 r.
3. Nieprawidłowości i braki w umowach powierzenia przetwarzania danych skutkują tym, iż Jednostka nie zapewnia odpowiedniego poziomu bezpieczeństwa danym osobowym powierzanym innym podmiotom. Zgodnie z zapisem art. 28 ust. 1 rozporządzenia RODO Administrator korzysta wyłącznie z usług podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia RODO. Brak odpowiednich zapisów w umowach powierzenia przetwarzania, gwarantujących przetwarzanie danych osobowych zgodnie z wymogami RODO skutkuje tym, iż odpowiedzialność za ewentualne błędy i naruszenia występujące po stronie Podmiotu Przetwarzającego, spoczywa na Administratorze. Brak zapisów zobowiązujących Podmiot Przetwarzający do poinformowania Administratora o wystąpieniu naruszenia ochrony danych po stronie przetwarzającego, może skutkować tym, iż Administrator nie będzie w stanie zrealizować w prawidłowy sposób zgłoszenia naruszenia danych, co za tym idzie może dojść do naruszenia kolejnych przepisów rozporządzenia RODO.

Narażą to Jednostkę na odpowiedzialność prawną oraz sankcje prawne przewidziane w rozdziale 11 Ustawy o Ochronie Danych Osobowych z dnia 10 maja 2018 r.

Zalecenia:

1. Należy dokonać dokładnego przeglądu Rejestru Czynności Przetwarzania oraz prawidłowo uzupełnić ww. rejestr. Szczególną uwagę należy zwrócić na pole „kategorie odbiorców" i wypełnić je zgodnie z wymaganiami art. 30 RODO oraz definicją odbiorcy znajdującą się w art. 4 pkt. 9 rozporządzenia RODO. Należy zweryfikować czy w rejestrze prawidłowo odnotowane są wszystkie czynności przetwarzania danych osobowych realizowane w Urzędzie.
2. Należy jak najszybciej dokończyć prowadzoną przez Inspektora Ochrony Danych analizę, której celem jest określenie czy Rejestr Wszystkich Kategorii Czynności Przetwarzania jest wymagany w Jednostce. Jeżeli okaże się, że jest wymagany należy go niezwłocznie wdrożyć.
3. Należy dokonać przeglądu wszystkich obowiązujących umów przetwarzania danych osobowych zawartych przez Gminę Masłów. Umowy, które nadal obowiązują a nie spełniają wymagań określonych w rozporządzeniu RODO i nie są zgodne z wzorem znajdującym się w załączniku nr 16 do Polityki Ochrony Danych należy poprawić i ponownie podpisać tak, aby zawierały zapisy gwarantujące prawidłowe przetwarzanie danych osobowych przez Podmioty, którym Gmina powierzyła dane osobowe.

7.3. Środki techniczne i organizacyjne stosowane do zapewnienia bezpieczeństwa informacji i danych osobowych

7.3.1. Środki techniczne i organizacyjne stosowane do zapewnienia bezpieczeństwa danych osobowych

Kryteria oceny stanu faktycznego:

Art. 32 Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) nazywane dalej Ogólnym rozporządzeniem o ochronie danych osobowych lub RODO).

Ustalenia stanu faktycznego:

1. W Urzędzie Gminy w Masłowie kwestie związane z zapewnieniem bezpieczeństwa danych osobowych reguluje dokument Polityki Ochrony Danych Osobowych. W Jednostce nie została opracowana odrębna instrukcja Zarządzania Systemem Informatycznym Służącym do przetwarzania danych osobowych. Wszystkie regulacje i procedury dotyczące bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych zostały opisane w Polityce Ochrony Danych.

   Polityka zawiera:

   1) W załączniku nr 13 - opis środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzanym danym, w którym znajdują się:
      a) Informacje o zastosowanych zabezpieczeniach budynku Jednostki;
      b) Opis obszaru przetwarzania danych osobowych;
      c) Opis procedury uzyskania upoważnienia do otwierania głównych drzwi wejściowych do budynku;
      d) Opis procedury otwierania budynku oraz pomieszczeń biurowych przez upoważnione osoby;
      e) Procedurę zakończenia pracy w Urzędzie;
      f) Wykaz systemów informatycznych służących do przetwarzania danych osobowych;
      g) Procedurę postępowania z kluczami do pomieszczeń biurowych;
      h) Informację dotyczącą zgody Administratora na przebywania pracowników w pomieszczeniach Jednostki poza godzinami pracy Urzędu;
      i) Procedurę tworzenia kopii zapasowych danych osobowych przetwarzanych w formie elektronicznej. Procedura ta jest opisana w bardzo ogólny sposób. Znajdują się w niej jedynie informacje o częstotliwości wykonywania kopii zapasowych, ogólnie wskazany zakres danych, z których tworzona jest kopia, sposób wykonania oraz rodzaj nośnika, na który jest tworzona kopia. W procedurze wskazano Informatyka jako osobę odpowiedzialną za wykonie kopii zapasowej oraz miejsce jej przechowywania (Serwerownia). Z informacji uzyskanych od Informatyka wynika, iż kopie bezpieczeństwa wykonywane są na dysku NAS umiejscowionym w serwerowni. Dodatkowo na płytę chowaną do sejfu w odrębnym pomieszczeniu archiwizowane są raz w tygodniu: Bazy danych programu dziedzinowego PUMA, Bazy danych programów finansowych i płacowych (Bestia, Płatnik), logi serwera domenowego, pliki konfiguracyjne urządzeń sieciowych (UTM, NAS Routery). Z powyższych informacji

wynika, że procedura wykonywania kopii znajdująca się w Polityce Ochrony Danych, nie w pełni opisuje realne działania wykonywane przez Informatyka.

2) W rozdziale nr 9 - obowiązki użytkowników systemu informatycznego dotyczące polityki „czystego biurka", polityki „czystego ekranu", zakazie podłączania urządzeń elektrycznych do listew zasilających sprzęt komputerowy. Znajdują się tam również zapisy dotyczące niszczenia niepotrzebnych dokumentów w niszczarkach, nie pozostawiania osób postronnych w pomieszczeniach, w których przetwarzane są dane osobowe bez obecności pracowników.
3) Rozdział 10 zawiera procedury dotyczące postępowania z przenośnymi nośnikami danych oraz przenośnymi komputerami.
4) Rozdział 11 precyzuje sposoby, miejsca i okresy przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników, na których znajdują się kopie zapasowe.
5) W rozdziale nr 12 zostały określone zasady pracy w systemach informatycznych. Rozdział ten opisuje następujące procedury:
   a) Procedurę nadawania i odbierania uprawnień użytkownikom systemu informatycznego;
   b) Metody i środki uwierzytelniania w systemach informatycznych oraz procedury związane z ich zarządzaniem i użytkowaniem. Procedury określają sposoby uwierzytelniania użytkowników, zasady tworzenia i przydzielania identyfikatorów/loginów, zasady dotyczące haseł dostępu do systemów informatycznych;
   c) Sposoby zabezpieczenia systemu informatycznego, w której znajdują się zapisy dotyczące:
      - stosowania oprogramowania antywirusowego,
      - sprawdzania komputerów pod kątem występowania szkodliwego oprogramowania,
      - obowiązków informatyka dotyczących nadzoru nad aktualizacją oprogramowania antywirusowego,
      - obowiązków użytkowników dotyczących zawiadamiania Informatyka o komunikatach systemu informatycznego, które sygnalizują o możliwości wystąpienia szkodliwego oprogramowania;
   d) Procedurę wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. Procedura ta jest bardzo ogólna, zawiera jedynie zapis, że za wykonanie przeglądów odpowiedzialny jest Informatyk. Brakuje w niej

wskazania częstotliwości wykonywania przeglądów lub kryteriów jej określania. Nie wskazano w niej również sposobu dokumentowania wykonywanych przeglądów;

e) Zasady bezpiecznego użytkowania sprzętu IT, które regulują kwestie związane z bezpiecznym korzystaniem ze sprzętu IT będącym własnością Jednostki. Znajdują się tam zapisy zakazujące użytkownikom systemu samodzielnych modyfikacji sprzętu komputerowego, instalowania dodatkowych urządzeń oraz podłączania do systemu informatycznego niezatwierdzonych urządzeń. Jest tam również zapis, który zakazuje podłączania do systemu informatycznego Jednostki bez zgody Administratora prywatnego sprzętu IT (np. laptopów, telefonów, aparatów, nośników typu pendrive), również w celu wykonywania obowiązków służbowych. W tej części znajduje się również informacja o prawie Administratora do monitorowania sprzętu służbowego wykorzystywanego przez pracowników. Wskazano załącznik nr 15, jako wzór oświadczenia podpisywanego przez pracowników, w którym znajdują się informacje dotyczące zakresu monitorowania stanowisk komputerowych;

f) Zasady korzystania z oprogramowania, które pozwalają na korzystanie przez pracowników jedynie z programów dopuszczonych do używania w Jednostce. Znajduje się tam zapis bezwzględnie zakazujący użytkownikom systemu instalowania i używania oprogramowania innego, niż przekazane lub udostępnione przez Administratora;

g) Zasady korzystania z Internetu, które określają cele i sposoby korzystania z Internetu przez pracowników Jednostki. Znajduje się tam zapis informujący pracowników o prawie Administratora do kontrolowania sposobu korzystania z Internetu przez Użytkowników;

h) Zasady korzystania z poczty elektronicznej, które zobowiązują pracowników do wykorzystywania służbowych adresów email jedynie w celu prowadzenia korespondencji związanej z działalnością Jednostki. W tej procedurze określono również kilka zasad dotyczących obsługi poczty elektronicznej;

i) Zasady dotyczące korzystania z bankowości elektronicznej przeznaczone dla pracowników, którzy w ramach obowiązków służbowych korzystają z takich narzędzi. Zasady określają w kilku zdaniach najważniejsze kwestie związane z bezpiecznym używaniem systemu bankowości elektronicznej.

6) Sposoby postępowania z dokumentami papierowymi zawierającymi dane osobowe, regulują kwestie zabezpieczenia, drukowania, przechowywania i niszczenia dokumentacji papierowej zawierającej dane osobowe. Zostały one opisane w rozdziale nr 13.

7) Przesyłanie dokumentów zawierających dane osobowe za pośrednictwem poczty elektronicznej jest opisane w rozdziale nr 14. Znajdują się tam zapisy zobowiązujące pracowników Jednostki do zastosowania środków ochrony kryptograficznej (szyfrowania) w odniesieniu do dokumentów zawierających dane osobowe przesyłanych pocztą elektroniczną.

2. Z informacji uzyskanych z list kontrolnych wypełnionych przez Informatyka urzędu Pana [redacted] wynika iż:

1) W Jednostce zastosowano mechanizmy uwierzytelniania użytkowników zarówno w systemach operacyjnych jak i systemach dziedzinowych – dwupoziomowy mechanizm uwierzytelniania.
2) W celu zabezpieczenia dostępu systemów informatycznych jednostek podległych do baz danych znajdujących się na serwerach w Urzędzie zastosowano szyfrowane, bezpieczne połączenia IPsec VPN.
3) Zastosowano kontrolę dostępu pomiędzy siecią lokalna Jednostki a Internetem realizowaną za pomocą urządzenia UTM Stormshield U30S-A, które ma na bieżąco aktualizowane oprogramowanie firewall i IPS.
4) Istnieje możliwość podłączenia nieautoryzowanego urządzenia do sieci lokalnej, jednak urządzenie takie ma ograniczony dostęp do zasobów sieci i Internetu. Prowadzony jest nadzór urządzeń podłączonych do sieci przez administratora. Stosowane są mechanizmy filtrowania adresów fizycznych MAC w celu uzyskania dostępu do sieci.
5) Wszystkie stacje robocze i serwery są zabezpieczone za pomocą oprogramowania antywirusowego z bieżącą aktualizacją baz szkodliwego oprogramowania.
6) Wszystkie serwery oraz większość stanowisk komputerowych posiada zasilacze awaryjne UPS.
7) W celu zabezpieczenia informacji przed ujawnieniem ich osobom postronnym zastosowano ograniczony dostęp do monitorów, każdy komputer posiada login i hasło, drukarka sieciowa zabezpieczona jest hasłem.
8) Pracownicy Jednostki nie mają możliwości zmiany ustawień lub instalacji oprogramowania na stacjach roboczych. Działania takie wymagają autoryzacji Informatyka.
9) W jednostce ustalono zasady postępowania z informacjami, których celem jest minimalizacja wystąpienia ryzyka kradzieży informacji, pkt. 10 i 11 Polityki Ochrony Danych zawiera procedury dotyczące korzystania z przenośnych nośników danych i komputerów przenośnych.
10) W jednostce wdrożona jest „polityka kluczy", która jest częścią Polityki Ochrony Danych.

Słabości/Ryzyka:

1. Brak precyzyjnej procedury tworzenia, przechowywania i testowania kopii zapasowych niesie za sobą ryzyko wystąpienia nieprawidłowości w zabezpieczeniu danych. Rozbieżność między procedurą wykonywania kopii opisaną w Polityce Ochrony Danych a realnym wykonywaniem kopii przez Informatyka oraz dodatkowy brak dokumentacji potwierdzającej wykonanie kopii, niesie za sobą ryzyko wystąpienia problemów w przypadku konieczności odtworzenia danych z kopii przez inną osobę niż Informatyk. W przypadku nieobecności informatyka mogą wystąpić problemy z prawidłowym zlokalizowaniem i identyfikacja właściwej kopii, co może spowodować znaczne wydłużenie czasu odtwarzania danych.

   Z informacji uzyskanych od Informatyka wynika, iż kopie zapasowe testowane są okazjonalnie, co może skutkować tym, że w przypadku wystąpienia awarii odtworzenia danych z kopii zapasowych może okazać się niemożliwe z powodu błędnego jej wykonania. Skutkiem tego może być poważny incydent związany z utratą danych.
2. Opisanie procedury wykonywania przeglądów i konserwacji systemów jednym zdaniem, które wskazuje Informatyka jako osobę odpowiedzialną za ich wykonanie niesie za sobą ryzyko wystąpienia nieprawidłowości podczas wykonywania tych czynności. Brak przeglądów i konserwacji bądź nie wykonanie ich w wymaganym czasie niesie za sobą ryzyko wystąpienia awarii sprzętu lub systemu informatycznego. Skutkiem tego może być czasowa lub stała utrata dostępu do danych.

Zalecenia:

1. Należy zweryfikować i poprawić opis procedury tworzenia kopii zapasowych tak, żeby odzwierciedlał realne działania wykonywane przez Informatyka w tym zakresie. Należy również stworzyć procedury określające sposób i częstotliwość testowania wykonywanych kopii.

   Procedury wykonywania i testowania kopii powinny również zawierać informacje o sposobie dokumentowania czynności związanych z prawidłowym bądź nieprawidłowym wykonaniem lub testowaniem kopii zapasowych.
2. Należy zmodyfikować procedury wykonywania przeglądów i konserwacji systemów i nośników danych tak, żeby określała zakres oraz częstotliwość jej wykonywania. W procedurze należy również zamieścić zapisy określające sposób dokumentowania wykonania przeglądów i konserwacji systemów i nośników danych.
3. Zaleca się dokonanie przeglądu stanowisk komputerowych pod względem ich zabezpieczenia przed awarią zasilania (wyposażenie w zasilacze awaryjne UPS). Należy zweryfikować czy na wszystkich stanowiskach, na których awaria zasilania może spowodować utratę danych

zastosowano zasilacze awaryjne UPS. W przypadku stwierdzenia, że istnieje możliwość utraty danych na skutek awarii zasilania należy zabezpieczyć zagrożone systemy poprzez zastosowanie zasilaczy awaryjnych.

7.3.2. Środki techniczne i organizacyjne stosowane do zapewnienia bezpieczeństwa informacji

Kryteria oceny stanu faktycznego:

§20 ust. 2 pkt. 7-12 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2016 poz.113), nazywanym dalej rozporządzeniem KRI.

Ustalenia stanu faktycznego:

1. W Jednostce nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami §20 ust. 1 rozporządzenia KRI oraz nie wdrożono Polityki Ochrony Informacji, która regulowałaby kwestie związane z przetwarzaniem wszystkich kategorii informacji. W Urzędzie Gminy w Masłowie została wdrożonych część regulacji wymaganych rozporządzeniem KRI. Są one opisane w Polityce Ochrony Danych i formalnie dotyczą jedynie przetwarzania danych osobowych, jednak w opinii audytora ich stosowanie zabezpiecza również częściowo lub całościowo informacje, które nie są danymi osobowymi.
2. Informatyk Pan [redacted] w listach kontrolnych udzielił następujących wyjaśnień dotyczących działań wymaganych rozporządzeniem KRI, które są realizowane w Urzędzie Gminy w Masłowie.
    1) Zastosowano odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych polegający na:
        a) dbałości o aktualizację oprogramowania,
        b) minimalizowanie ryzyka utraty informacji w wyniku awarii,
        c) ochronie przed błędami, utratą informacji oraz nieuprawniona modyfikacją,
        d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa,
        e) zapewnienia bezpieczeństwa plików systemowych,
        f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności systemów teleinformatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwe naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

2) Operacje dostępu do systemu przez użytkowników z uprawnieniami administracyjnymi podlegają wiarygodnemu dokumentowaniu poprzez zapisy logów systemu Windows Server.

3) Rozliczalność operacji wykonywanych w systemach teleinformatycznych podlega wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów poprzez zapisy logów operacji na danych wykonywanych w systemach dziedzinowych.

4) Operacje na danych podlegających ochronie prawnej podlegają wiarygodnemu dokumentowaniu w postaci elektronicznych zapisów w dziennikach systemów poprzez logi operacji na danych wykonywane w systemach dziedzinowych.

5) W umowach na łącza internetowe nie określono maksymalnego czasu przerwy w dostępie do Internetu. W Jednostce nie określono akceptowalnego czasu braku dostępu do Internetu.

6) W Jednostce ustalono właściwą formę kontaktu z operatorami telekomunikacyjnymi, dostawcami Internetu, dostawcami usług wsparcia technicznego, dostawcami sprzętu i oprogramowania i innymi instytucjami na wypadek zaistnienia nieprzewidzianych zdarzeń.

7) W celu fizycznego zabezpieczenia ochrony informacji w Jednostce zastosowano:
   - monitoring wizyjny wejścia budynku,
   - czujniki ruchu (alarm) z automatycznym powiadomieniem firmy ochroniarskiej w przypadku wykrycia włamania,
   - wydzieloną serwerownią z ograniczonym dostępem (drzwi metalowe bez certyfikatu),
   - serwerownia wyposażona w klimatyzację i gaśnicę do elektroniki.

8) Okablowanie służące przesyłaniu danych jest zabezpieczone przed zniszczeniem.

9) Wszelkie dane, informacje pochodzące z zewnętrznej, niezabezpieczonej sieci są sprawdzane pod kątem wystąpienia wirusów i innego szkodliwego oprogramowania.

10) Istnieją środki kontroli zabezpieczające przed użyciem/wystąpieniem na stanowiskach komputerowych szkodliwego i nielicencjonowanego oprogramowania.

Słabości/Ryzyka:

1. Brak zapisów określających maksymalny czas przerwy w dostępie do Internetu, może skutkować tym, iż w przypadku wystąpienia awarii łącza wystąpią problemy z realizacją zadań i zobowiązań przez Jednostkę.
2. W opinii audytora zabezpieczenie serwerowni jest niewystarczające w odniesieniu do zagrożeń dotyczących tego pomieszczenia. Pomieszczenie serwerowni jest pomieszczeniem specyficznym - szczególnie narażonym na wystąpienie pożaru. Brak systemu wykrywania pożaru (czujnika dymu) z powiadomieniem służb zewnętrznych lub firmy ochroniarskiej powoduje znaczne ryzyko wystąpienia dużych strat w przypadku pożaru serwerowni. Gdyby do pożaru doszło w godzinach nocnych lub w dniu, w którym Urząd jest zamknięty, czas od wystąpienia pożaru do czasu jego wykrycia może być na tyle długi, że zniszczeniu ulegnie całe pomieszczenie serwerowni wraz ze sprzętem oraz informacjami przechowywanymi na urządzeniach tam zlokalizowanych. Również niecertyfikowane drzwi powodują wzrost ryzyka zniszczenia tego pomieszczenia w przypadku wystąpienia pożaru na zewnątrz serwerowni, gdyż może on się przedostać przez nieodpowiednie drzwi.
3. Mimo, iż z informacji uzyskanych od Informatyka Pana [redacted] wynika, że Jednostka realizuje cześć wymagań dotyczących zapewnienia ochrony przetwarzanych informacji przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami określonymi w §20 rozporządzenia KRI, to fakt iż w Urzędzie nie wdrożono kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji naraża Jednostkę na konsekwencje związane z niezrealizowaniem obowiązujących przepisów prawa. Sam fakt spełniania części wymagań bez stworzenia i wdrożenia odpowiednich procedur określających sposoby ich realizacji i dokumentowania tylko częściowo spełnia wymagania rozporządzenia KRI.

Zalecenia:

1. Należy określić akceptowalny czas braku dostępu do Internetu i dostosować zapisy w umowach z jego dostawcami tak, aby gwarantowały odpowiedni czas przywrócenia łącza w przypadku jego awarii. Ryzyko związane z barkiem dostępu do Internetu można również minimalizować poprzez zastosowanie redundancji łącza - zapewnienie dostępu do Internetu od co najmniej dwóch różnych dostawców, którzy będą świadczyć usługę za pomocą różnych mediów transmisyjnych.

2. Należy wyposażyć pomieszczenie serwerowni w system wykrywania pożaru z powiadamianiem służb lub firmy ochroniarskiej oraz w certyfikowane drzwi antywłamaniowe o podwyższonej odporności ogniowej.
3. Zgodnie z §20 rozporządzenia KRI w Urzędzie Gminy w Masłowie należy stworzyć i wdrożyć System Zarządzania Bezpieczeństwem Informacji, który będzie zapewniał i dokumentował działania podejmowane przez Jednostkę w celu zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami i zakłóceniami.

8. Opinia audytora w sprawie adekwatności, skuteczności i efektywności kontroli zarządczej w obszarze ryzyka objętym zadaniem zapewniającym

Na podstawie przeprowadzonego zadania zapewniającego stwierdzono, że w badanym obszarze w ograniczonym stopniu funkcjonowała adekwatna, skuteczna i efektywna kontrola zarządcza.
W wyniku przeprowadzonego audytu, w opinii audytora mimo stwierdzonych słabości system kontroli zarządczej w obszarze audytowanym zapewnia realizację celów i zadań zgodnie z obowiązującymi przepisami prawa w sposób efektywny, oszczędny i terminowy, zatem audytor wydaje opinię pozytywną z zastrzeżeniami.
W celu zwiększenia adekwatności, skuteczności i efektywności kontroli zarządczej wskazane jest wprowadzenie rekomendacji opisanych w pkt. 9 niniejszego sprawozdania.

9. Zalecenia w zakresie działań mających na celu dostosowanie systemu zarządzania ochrona danych do przepisów RODO.

Dla wydanych w toku zadania audytowego zaleceń przyznano poziom **I** istotności – wskaźnik ważności niski, ustalenia o umiarkowanym znaczeniu, ich charakter i rozmiar dla audytowanej działalności nie stanowi zagrożenia, wymaga jednak podjęcia działania przez Kierownika komórki audytowanej:

System Zarządzania Bezpieczeństwem Informacji

1. Zgodnie z §20 rozporządzenia KRI należy opracować i ustanowić, wdrożyć i eksploatować, monitorować i przeglądać, utrzymywać i doskonalić System Zarządzania Bezpieczeństwem Informacji. System ten powinien zapewniać poufność, dostępność i integralność wszystkich informacji przetwarzanych w Urzędzie Gminy w Masłowie z uwzględnieniem takich atrybutów jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Niezbędnym elementem tego systemu powinna być Polityka Bezpieczeństwa Informacji, która będzie stanowić zbiór reguł, zasad i procedur stosowanych przez Urząd Gminy w Masłowie w celu osiągnięcia

interoperacyjności oraz odpowiedniego poziomu bezpieczeństwa w odniesieniu do wszystkich przetwarzanych informacji (nie tylko danych osobowych). Ponieważ w Jednostce opracowano i wdrożono system ochrony danych osobowych, który reguluje wiele obszarów opisanych w rozporządzenia KRI można rozważyć dostosowanie tego systemu do ochrony nie tylko danych osobowych, ale również pozostałych informacji. W opinii audytora takie działanie jest zasadne i mniej pracochłonne niż tworzenie systemu zarządzania bezpieczeństwem informacji od podstaw. Należy rozważyć dostosowanie/zmianę dokumentów i procedur dotyczących przetwarzania danych osobowych w taki sposób, aby dotyczyły wszystkich informacji przetwarzanych w Jednostce (w tym danych osobowych). W przypadku obszarów, które nie są objęte procedurami stosowanymi w Jednostce, a są wymagane rozporządzeniem KRI, należy stworzyć i wdrożyć procedury, które będą regulowały brakujące obszary związane z bezpieczeństwem informacji. Zbiór wszystkich regulacji stworzy Politykę Ochrony Informacji, która powinna stanowić kluczowy element Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy w Masłowie.

2. Zgodnie z §20 ust. 2 pkt. 6 należy zapewnić szkolenia osób zaangażowanych w przetwarzanie informacji. Tematyka szkoleń powinna być dostosowana do wymagań stawianych przez rozporządzenie KRI, dotyczących przetwarzania wszystkich rodzajów informacji (nie tylko danych osobowych). Szkolenia pracowników należy dokumentować poprzez odnotowanie listy przeszkolonych pracowników, daty szkolenia oraz zakresu szkolenia.

Obszar Ochrony Danych Osobowych

1. Należy dokonać dokładnego przeglądu Rejestru Czynności Przetwarzania oraz prawidłowo uzupełnić ww. rejestr. Szczególną uwagę należy zwrócić na pole „kategorie odbiorców" i wypełnić je zgodnie z wymaganiami art. 30 RODO oraz definicją odbiorcy znajdującą się w art. 4 pkt. 9 rozporządzenia RODO. Należy zweryfikować czy w rejestrze prawidłowo odnotowane są wszystkie czynności przetwarzania danych osobowych realizowane w Urzędzie.
2. Należy jak najszybciej dokończyć prowadzoną przez Inspektora Ochrony Danych analizę, której celem jest określenie czy Rejestr Wszystkich Kategorii Czynności Przetwarzania jest wymagany w Jednostce. Jeżeli okaże się, że jest wymagany należy go niezwłocznie wdrożyć.
3. Należy dokonać przeglądu wszystkich obowiązujących umów przetwarzania danych osobowych zawartych przez Gminę Masłów. Umowy, które nadal obowiązują a nie spełniają wymagań określonych w rozporządzeniu RODO i nie są zgodne z wzorem znajdującym się w załączniku nr 16 do Polityki Ochrony Danych należy poprawić i ponownie podpisać tak, aby zawierały

zapisy gwarantujące prawidłowe przetwarzanie danych osobowych przez Podmioty, którym Gmina powierzyła dane osobowe.

Środki techniczne i organizacyjne stosowane do zapewnienia bezpieczeństwa danych osobowych

1. Należy zweryfikować i poprawić opis procedury tworzenia kopii zapasowych tak, żeby odzwierciedlał realne działania wykonywane przez Informatyka w tym zakresie. Należy również stworzyć procedury określające sposób i częstotliwość testowania wykonywanych kopii.
   Procedury wykonywania i testowania kopii powinny również zawierać informacje o sposobie dokumentowania czynności związanych z prawidłowym bądź nieprawidłowym wykonaniem lub testowaniem kopii zapasowych.
2. Należy zmodyfikować procedury wykonywania przeglądów i konserwacji systemów i nośników danych tak, żeby określała zakres oraz częstotliwość jej wykonywania. W procedurze należy również zamieścić zapisy określające sposób dokumentowania wykonania przeglądów i konserwacji systemów i nośników danych.
3. Zaleca się dokonanie przeglądu stanowisk komputerowych pod względem ich zabezpieczenia przed awarią zasilania (wyposażenie w zasilacze awaryjne UPS). Należy zweryfikować czy na wszystkich stanowiskach, na których awaria zasilania może spowodować utratę danych zastosowano zasilacze awaryjne UPS. W przypadku stwierdzenia, że istnieje możliwość utraty danych na skutek awarii zasilania należy zabezpieczyć zagrożone systemy poprzez zastosowanie zasilaczy awaryjnych.

Środki techniczne i organizacyjne stosowane do zapewnienia bezpieczeństwa informacji

1. Należy określić akceptowalny czas braku dostępu do Internetu i dostosować zapisy w umowach z jego dostawcami tak, aby gwarantowały odpowiedni czas przywrócenia łącza w przypadku jego awarii. Ryzyko związane z barkiem dostępu do Internetu można również minimalizować poprzez zastosowanie redundancji łącza - zapewnienie dostępu do Internetu od co najmniej dwóch różnych dostawców, którzy będą świadczyć usługę za pomocą różnych mediów transmisyjnych.
2. Należy wyposażyć pomieszczenie serwerowni w system wykrywania pożaru z powiadamianiem służb lub firmy ochroniarskiej oraz w certyfikowane drzwi antywłamaniowe o podwyższonej odporności ogniowej.
3. Zgodnie z §20 rozporządzenia KRI w Urzędzie Gminy w Masłowie należy stworzyć i wdrożyć System Zarządzania Bezpieczeństwem Informacji, który będzie zapewniał i dokumentował

działania podejmowane przez Jednostkę w celu zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami i zakłóceniami.

10. Informacje końcowe

Audytowany, w terminie 14 dni kalendarzowych od dnia otrzymania sprawozdania, ustala sposób i termin realizacji zaleceń oraz wyznacza osoby odpowiedzialne za realizację zaleceń, powiadamiając o tym na piśmie audytora wewnętrznego i kierownika jednostki.

W przypadku odmowy realizacji zaleceń audytowany przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania sprawozdania, pisemne stanowisko kierownikowi jednostki i audytorowi wewnętrznemu.

W przypadku, o którym mowa w punkcie powyższym, kierownik jednostki podejmuje decyzję dotyczącą realizacji zaleceń, informując o tym audytowanego i kierownika komórki audytu wewnętrznego.

Załączniki:

1. Załącznik nr 1 do sprawozdania z zadnia zapewniającego „Bezpieczeństwo Informacji w Urzędzie Gminy Masłów" Lista zgodności z KRI – na 5 stronach - strony od 31 do 35 niniejszego sprawozdania.
2. Załącznik nr 2 do sprawozdania z zadnia zapewniającego „Bezpieczeństwo Informacji w Urzędzie Gminy Masłów" Lista pytań do audytu – strony od 36 do 50 niniejszego sprawozdania.

Imię i nazwisko audytora wewnętrznego przeprowadzającego zadanie audytowe oraz jego podpis:

[redacted]

MF nr 2108 AUDYTOR WEWNĘTRZNY [redacted]

.....

Data sporządzenia – **31.01.2019** r.

Sporządzono w czterech jednobrzmiących egzemplarzach na 50 stronach, które otrzymują:

1. Wójt Gminy Masłów,
2. Sekretarz Gminy Masłów
3. Informatyk Urzędu Gminy Masłów
4. a/a.