Rzeszów, dnia 8 kwietnia 2020 r.

Urząd Gminy Goworowo
ul. Ostrołęcka 21
07-440 Goworowo

AW.G.1.2020

Egz. Nr 1

Sprawozdanie
z zadania audytowego przeprowadzonego na rzecz Urzędu Gminy Goworowo

Temat: *„Funkcjonowanie systemu bezpieczeństwa teleinformatycznego w Urzędzie Gminy w Goworowie”.*

Audytor wewnętrzny:

Marek Żuczek

Zadanie audytowe przeprowadzono zgodnie z międzynarodowymi standardami audytu wewnętrznego

Rzeszów 2020

Zadanie audytowe zostało przeprowadzone zgodnie z planem audytu wewnętrznego na 2020 rok w Urzędzie Gminy Goworowo

Audytor wewnętrzny postanowił objąć zadaniem audytowym następujące obszary ryzyka:

1. Adekwatność i aktualność regulacji wewnętrznych w zakresie dotyczącym ochrony danych osobowych;
2. Podjęte działania w związku z koniecznością wdrożenia ogólnego rozporządzenia o ochronie danych tzw. RODO;
3. Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4. Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
5. Zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;
6. Ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
7. Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych.

Termin, w którym przeprowadzono zadanie audytowe:
luty/marzec 2020 r.

Badany okres:
2018-2020.

Kryteria oceny:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 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, nazywane ogólnym rozporządzeniem o ochronie danych osobowych (RODO)[1];

[1] Dz.U. UE z 2016 r. L119/1.

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[2];
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[3];
- 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[4];
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[5];
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez Administratora Bezpieczeństwa Informacji[6];
- Zarządzenie nr 42/2018 Wójta Gminy Goworowo z dnia 29.06.2018 r. *„w wprowadzenia Polityki Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym”;*
- Polityka Ochrony Danych Osobowych w Urzędu Gminy Goworowo;
- Instrukcja zarządzania systemem informatycznym Urzędu Gminy Goworowo.

Zakres przedmiotowy zadania audytowego:

Zakresem przedmiotowym zadania audytowego objęto:

- kwestię wdrożenia ogólnego rozporządzenia o ochronie danych osobowych RODO,
- analizę systemu zarządzania bezpieczeństwem informacji,
- kwestię podziału obowiązków osób zaangażowanych w zarządzanie bezpieczeństwem informacji,
- kwestię ochrony danych osobowych.

[2] Dz. U.z 2018 r. poz. 1000 ze zm.
[3] t. jedn., Dz. U. z 2016 r. poz. 922.
[4] t. jedn., Dz. U. z 2016 r. poz. 113.
[5] Dz. U. z 2004 r. Nr 100 poz. 1024.
[6] Dz. U. z 2015 r. poz. 745.

Podjęte działania i zastosowane techniki przeprowadzania zadania audytowego:

W trakcie zadania audytowego została przeprowadzona rozmowa z Sekretarzem Gminy oraz informatykiem pełniącym funkcję ASI tj. - osobami bezpośrednio zaangażowanymi w proces zarządzania bezpieczeństwem informacji. Sporządzono listę pytań kontrolnych, przeprowadzono testy zgodności i testy przeglądowe.

Celem zadania audytowego było zapewnienie Wójta, że:

1. Obowiązujące w Urzędzie Gminy mechanizmy kontrolne i schematy działania dotyczące ochrony danych osobowych są zgodne z przepisami powszechnie obowiązującego prawa;
2. Urząd Gminy podjął odpowiednie działania w związku z koniecznością wdrożenia ogólnego rozporządzenia o ochronie danych osobowych - RODO;
3. Funkcjonujący w Urzędzie Gminie system bezpieczeństwa informacji gwarantuje optymalną ochronę informacji przed nieautoryzowanym dostępem;
4. Zastosowane w systemie mechanizmy zarządzania informacją, jak również mechanizmy kontroli zarządczej, są adekwatne do znaczenia audytowanych procesów w ramach funkcjonowania całej jednostki.

Tło informacyjne:

Od 25 maja 2018 r. z uwagi na wejście do stosowania nowych przepisów regulujących zagadnienia ochrony danych osobowych oraz wejście w życie nowej ustawy o ochronie danych osobowych tracą moc wcześniej obowiązujące wymagania dotyczące dokumentacji przetwarzania danych osobowych. Obecnie wszelkie wymagania w powyższym zakresie powinny być zgodne przede wszystkim z wymaganiami określonymi w:

1. Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 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 nazywanego ogólnym Rozporządzeniem o ochronie danych osobowych (RODO);
2. Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r., poz. 1000 ze zm.).

Zauważyć jednak należy, że wyżej wymienione akty prawne, w tym RODO, nie zawierają praktycznie żadnych wytycznych odnoszących się do sposobu prowadzenia

dokumentacji przetwarzania danych osobowych, jak również jej zawartości. Nie oznacza to jednak, że po 25 maja 2018 r. administrator danych nie jest zobligowany do posiadania żadnej dokumentacji w tym zakresie. RODO nie określa formalnych wymagań dotyczących dokumentacji przetwarzania danych osobowych dając tym samym dużą swobodę w tym zakresie administratorom danych. Brak w RODO wymagań formalnych w zakresie prowadzenia dokumentacji przetwarzania danych osobowych na wzór nieobowiązującego już rozporządzenia ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych (...) **nie oznacza, że od 25 maja 2018 r. administrator nie jest zobowiązany do prowadzenia dokumentacji, w której określone byłyby zasady i procedury dotyczące przetwarzania danych osobowych zgodnie z przyjętymi rozwiązaniami prawnymi, organizacyjnymi i technicznymi.**

W nowym systemie prawnym dotyczącym przetwarzania danych osobowych administrator danych w większości obszarów dowolnie może kształtować i opisywać rozwiązania dotyczące przyjętych zasad i procedur przetwarzania. Wśród obszarów, w odniesieniu do których w RODO nakreślono jednak pewne wymagania formalne dotyczące zakresu dokumentowania, pozostały takie zagadnienia jak:

- prowadzenie rejestru czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;
- zgłaszanie naruszenia ochrony danych do organu nadzorczego (UODO) – art. 33 ust 3. RODO;
- prowadzenie wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO;
- zawartość raportu dokumentującego wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7 RODO.

RODO nie wymaga jednak, aby dokument zawierający wymienione wyżej obligatoryjne elementy dokumentacji miał określona nazwę czy strukturę. Ważne jest tylko, aby administrator danych wykazał, że wymienione wyżej rejestry czy raporty posiadał i aby ich zawartość była zgodna z wskazanymi wyżej wymaganiami tj. odpowiednio w art. 30, art. 33 ust. 3 i 5 oraz art. 35 ust. 7 RODO. Należy pamiętać jednak, że wskazane w RODO wymagania wymienione w art. 30, art. 33 ust. 3 i 5 oraz art. 35 ust. 7 nie są jedynymi, jakie należy uwzględnić w dokumentacji przetwarzania. Są one jedynie specyficzne pod tym względem, że wskazany jest zakres informacji, jaki w danym obszarze powinien być uwzględniony. Decydujące znaczenie dla obszaru i zakresu informacji, jakie powinny być

zawarte w dokumentacji przetwarzania, ma wymóg wykazania przez administratora przestrzegania przepisów RODO, zawarty w art. 24, którego brzmienie jest następujące:

- Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, **administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać.** Środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
- Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych;
- Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Wymaganie zawarte art. 24 RODO stanowiące, że administrator powinien być w stanie wykazać przestrzeganie przepisów RODO, oznacza w praktyce, że sposób przetwarzania danych, związane z nim procedury, jak i zastosowane zabezpieczenia techniczne i organizacyjne, również powinny zostać zawarte w przedmiotowej dokumentacji – jako spełnienie obowiązku wykazania, że przestrzegane są wymagania RODO.

Zdaniem Audytora, nieprawdą jest, jak twierdzą wprost niektórzy eksperci, że RODO znosi „uciążliwy dotąd" obowiązek prowadzenia dokumentacji przetwarzania danych tj. dokumentacji, na którą składa się polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.

Obecnie, w nowym systemie prawnym dotyczącym przetwarzania danych osobowych, nie wymienia się dokumentów, jakie administrator powinien posiadać, aby wykazać zgodność realizowanych czynności przetwarzania, poza elementami wymienionymi w rozdziale 1. Z treści art. 24 ust 1 RODO wynika jednak, że administrator danych ma być w stanie wykazać całościowo zgodność przetwarzania danych. W praktyce oznacza to, że administrator ma obowiązek wykazać, że:

1. stosuje się do ogólnych zasad przetwarzania określonych w art. 5 RODO;
2. zapewnia, aby dane przetwarzane były zgodnie z prawem – art. 6 – 11 RODO;
3. zapewnia, aby przestrzegane były prawa osób, których dane są przetwarzane – art. 12-23 RODO;

4. zapewnia wypełnianie ogólnych obowiązków w zakresie przetwarzania danych ciążących na administratorze i podmiocie przetwarzającym – art. 24 – 31 RODO;
5. zapewnia bezpieczeństwo przetwarzania danych uwzględniając charakter, zakres, kontekst i cele przetwarzania danych – art. 32- 36 RODO;
6. zapewnia kontrolę nad przetwarzaniem danych w postaci monitorowania przestrzegania przepisów i przyjętych procedur przetwarzania przez Inspektora Ochrony Danych lub podmioty certyfikujące, czy monitorujące przestrzeganie przyjętych kodeksów postępowania – art. 27- 43;
7. stosuje się do wymagań w zakresie przekazywania danych do państw trzecich i instytucji międzynarodowych – art. 44 – 49 RODO.

Należy jednak zaznaczyć, że zgodnie z art. 24 oraz art. 32 RODO przy wykonywaniu wyżej wymienionych obowiązków w zakresie zapewniania zgodności należy uwzględniać stan wiedzy technicznej, koszty, charakter, zakres, kontekst, cele przetwarzania a także ryzyka, na jakie są narażone przetwarzane dane.

Obowiązkowa dokumentacja (do 25.05.2018 r.), na którą składały się polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, z powodzeniem mogła być wykorzystana w celu stworzenia dokumentacji, której celem będzie wykazanie zgodności realizowanych procesów przetwarzania z wymaganiami RODO. Obowiązek wykazania, przestrzegania i stosowania przepisów RODO wynikający z art. 24 RODO nie określa bowiem, w jaki sposób, poprzez jakie dokumenty czy inne instrumenty zarządzania, powinien on być zrealizowany. Przepis art. 24 RODO stanowi jedynie, że administrator ma wykazać, że wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO. Opracowana dokumentacja, powinna zatem opisywać zastosowane w powyższym celu procedury i środki techniczne. Jeśli zatem prowadzona wg poprzednich wymagań dokumentacja zawierała wymagane elementy, takie jak inwentaryzacja zasobów informacyjnych, opis przepływu danych między systemami czy specyfikacje środków organizacyjnych i technicznych zastosowanych do ochrony przetwarzanych danych (czego wymagała polityka bezpieczeństwa) to w pełni można je przenieść do nowej dokumentacji. Nie ma również przeszkód, aby do problemu nowej dokumentacji, która będzie spełniała nowe wymagania, o których mowa wyżej, podejść w sposób odwrotny tj. uzupełnić dotychczas stosowaną dokumentacje o nowe elementy wymienione w RODO. Należy dodatkowo pamiętać, że dokumentując przyjęte procedury i wymagania dotyczące przetwarzania danych osobowych, zgodnie z art. 32 ust. 1 RODO, powinniśmy mieć na uwadze, aby przyjęte rozwiązania były

adekwatne do obecnego stanu wiedzy technicznej. Dotyczy to nie tylko wiedzy technicznej w zakresie dostępnych środków bezpieczeństwa, ale również wiedzy w zakresie systemów zarządzania bezpieczeństwem, do którego należą takie elementy jak standardy w zakresie zarządzania, dokumentowania zmian, konfiguracji i innych elementów, które powinny być zawarte w dokumentacji przetwarzania.

Należy przy tym pamiętać również o innych obowiązujących wymaganiach prawnych nadal obowiązujących, takich jak wymagania określone w:

- ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jednolity Dz. U. z 2014 r. poz. 1114) oraz wydanemu do niej
- rozporządzeniu 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 (tekst jednolity Dz. U. z 2016 r. poz. 113).

W wyżej wymienionych dokumentach, w kontekście dokumentacji przetwarzania, warto zwrócić uwagę w szczególności na § 20 ust. 1 rozporządzenia, który stanowi, że:

„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". W odniesieniu natomiast do działań, jakie chcemy wykazać w kontekście wykazania dbałości o bezpieczeństwo przetwarzanych danych, należy skorzystać z zaleceń wymienionych w § 20 ust 2 rozporządzenia odnoszących się do zarządzania bezpieczeństwem, które stanowi, że powinno to być zapewniane poprzez:

1. zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2. utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4. podejmowanie 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;

5. bezzwłoczną zmiana uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
6. **zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:**
   - ✓ **zagrożenia bezpieczeństwa informacji,**
   - ✓ **skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,**
   - ✓ **stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;**
7. zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   - ✓ monitorowanie dostępu do informacji,
   - ✓ czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   - ✓ zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9. zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10. zawieranie w umowach serwisowych, podpisanych ze stronami trzecimi, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11. ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12. zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
    - ✓ dbałości o aktualizację oprogramowania,
    - ✓ minimalizowaniu ryzyka utraty informacji w wyniku awarii,
    - ✓ ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
    - ✓ stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

- ✓ zapewnieniu bezpieczeństwa plików systemowych,
- ✓ redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
- ✓ niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
- ✓ kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

13. **bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;**
14. **zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.**

Zdaniem Audytora dokumentacja przetwarzania zgodnie z RODO powinna również zawierać instrukcje zarządzania systemami informatycznymi. RODO nie określa wprost, jak należy udokumentować organizację przetwarzania i zarządzanie bezpieczeństwem przetwarzanych danych, w tym instrukcji zarządzania systemami informatycznymi. Wymaga jednak, aby zastosowane środki bezpieczeństwa i wszystkie podejmowane w tym zakresie działania można było wykazać. Jak stanowi art. 24 RODO, wykazując zgodność przetwarzania z obowiązującymi wymaganiami należy uwzględnić: charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

Ponadto obowiązek prowadzenia dokumentacji przetwarzania danych wynika pośrednio również z art. 32 RODO dotyczącego bezpieczeństwa przetwarzania, który stanowi, że: „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym

prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku (...)."

Biorąc zaś pod uwagę fakt, że jednym z najważniejszych, powszechnie akceptowanych dokumentów prezentujących aktualny stan wiedzy technicznej w zakresie stosowania środków bezpieczeństwa i zarządzania bezpieczeństwem są m.in. normy ISO/IEC z serii 27000, w tym: norma PN-EN ISO/IEC 27001:2017 Technologia informacyjna - Techniki zabezpieczeń, oraz norma PN-EN ISO/IEC 27002:2017 Technika informatyczna - Technika bezpieczeństwa - Praktyczne zasady zabezpieczania informacji, warto zaznaczyć, że wyraźnie podkreśla się w nich fakt, że polityka bezpieczeństwa informacji powinna być: dostępna w formie udokumentowanej informacji, ogłoszona wewnątrz organizacji oraz dostępna dla zainteresowanych stron. Jeśli chodzi o zawartość dokumentacji przetwarzania, to należy mieć na uwadze zawarte m.in. w art. 24 i 32 RODO wymaganie wskazujące, że opracowana polityka bezpieczeństwa powinna uwzględniać zakres, kontekst i cele przetwarzania oraz ryzyka naruszenia praw i wolności, w tym prawdopodobieństwo ich wystąpienia. Odwołując się w powyższym zakresie do aktualnego stanu wiedzy, można się posłużyć z kolei normą PN-EN ISO/IEC 27002:2017, która zaleca w tym zakresie uwzględnić takie elementy, jak:

- ✓ zarządzanie aktywami (przetwarzanymi zbiorami danych);
- ✓ kontrole dostępu (rejestrowanie i wyrejestrowywanie użytkowników, zarządzanie hasłami, użycie uprzywilejowanych programów narzędziowych);
- ✓ środki ochrony kryptograficznej (polityka stosowania zabezpieczeń, zarządzanie kluczami);
- ✓ bezpieczeństwo fizyczne i środowiskowe oraz bezpieczeństwo eksploatacji (zarządzanie zmianami, zarządzanie pojemnością, zapewnienie ciągłości działania, rejestrowanie zdarzeń i monitorowanie);
- ✓ bezpieczeństwo komunikacji (zabezpieczenie, rozdzielenie sieci);
- ✓ pozyskiwanie, rozwój i utrzymywanie systemów;
- ✓ relacje z dostawcami (umowy, w tym umowy powierzenia przetwarzania);
- ✓ zarządzanie incydentami związanymi z bezpieczeństwem informacji;
- ✓ zarządzanie ciągłością działania;
- ✓ zgodność z wymaganiami prawnymi i umownymi.

Część z wymienionych wyżej elementów zgodnie z obowiązującymi dotychczas wymaganiami powinna być zawarta w prowadzonej dotychczas instrukcji zarządzania

systemami informatycznymi. Tak więc elementy te również należy wykorzystać dla wykazania w nowej dokumentacji zgodności, o której mowa art. 24 RODO.

Opis stanu faktycznego – nowa dokumentacja systemu zarządzania bezpieczeństwem informacji wdrożona w Urzędzie Gminy, dostosowana do RODO:

Tab. nr 1 Test - dokumentacja systemu zarządzania bezpieczeństwem informacji.

Sposób przeprowadzenia czynności audytowych:
- Analiza aktów wewnętrznych dot. bezpieczeństwa ochrony danych osobowych .
- Uzyskiwanie wyjaśnień i informacji od osób odpowiedzialnych za prawidłowe funkcjonowanie systemu bezpieczeństwa informacji oraz od innych pracowników jednostki.
- Zapoznawanie się z dokumentami służbowymi, na podstawie których można będzie dokonać ustalenia stanu faktycznego, np. zakresy obowiązków pracowników, plany szkoleń, protokoły przeprowadzonych szkoleń, wykaz pracowników, zapoznanych z aktami wewnętrznymi dotyczącymi bezpieczeństwa informacji, itp.

	TREŚĆ PYTANIA	*ODPOWIEDZI* TAK	NIE	*DOWÓD W PRZYPADKU ZAZNACZENIA "TAK"*	*UWAGI*
1	Czy określono zasady zarządzania bezpieczeństwem informacji przetwarzanych w jednostce ? Jeśli tak to: a) czy opracowano politykę bezpieczeństwa ochrony danych osobowych? b) czy opracowano dokumentację zarządzania systemem informatycznym służącym do przetwarzania danych osobowych? c) czy opracowano instrukcję postępowania w sytuacji naruszenia bezpieczeństwa informacji? d) Czy Wójt formalnie zatwierdził ww. dokumentację? e) czy zakomunikowano dokumentację pracownikom? f) czy i w jaki sposób zapewnia się, że pracownicy zapoznali się z polityką bezpieczeństwa i potwierdzili obowiązek jej przestrzegania? g) czy procedury wewnętrzne są tworzone w oparciu	Tak Tak Tak Tak Tak Tak Tak		Zarządzeniem NR 42/2018 z dnia 29.06.2018 r. Wójta Gminy Goworowo wdrożono Politykę Ochrony Danych oraz Instrukcję Zarządzania Systemem Informatycznym w Urzędzie Gminy Goworowo. W § 11 ww. Polityki opisano instrukcję postępowania w sytuacji naruszenia bezpieczeństwa informacji. Dokumentacja została zatwierdzona przez Wójta Gminy Goworowo. Dokumentacja została podana do wiadomości każdemu z pracowników Urzędu. W dokumentacji są stosowne - podpisane przez pracowników - oświadczenia o zapoznaniu się z dokumentacją z zakresu bezpieczeństwa informacji i potwierdzające obowiązek jej przestrzegania. W dokumentacji wskazana jest podstawa prawna, w oparciu o którą tworzono dokumentację	

	o przepisy prawa w zakresie bezpieczeństwa informacji?			w zakresie bezpieczeństwa informacji.	
2.	Czy dokumentacja dotycząca ochrony danych zawiera: a) definicje, zakres oraz znaczenie bezpieczeństwa ochrony danych osobowych? b) cele i zadania ? c) nawiązania do regulacji prawnych? d) zakresy obowiązków związanych z zarządzaniem bezpieczeństwem? e) określenie stosowanych zabezpieczeń z uwzględnieniem analizy ryzyka? f) odniesienia do dokumentów uzupełniających?	Tak Tak Tak Tak Tak Tak		W dokumentacji zawarto stosowne definicje. W postanowieniach ogólnych/wstępie opisano cele i zadania funkcjonowania polityki. Polityka bezpieczeństwa, Umowy cywilne z dnia 30.03.2018 r. oraz 28 marca 2019 r., w których zawarto zakres obowiązków IOD. Za bezpieczeństwo danych odpowiedzialny jest ADO oraz IOD, którzy sprawują nadzór nad przestrzeganiem postanowień polityki. W polityce uwzględniono szczegółowy wykaz stosowanych środków bezpieczeństwa, z uwzględnieniem analizy ryzyka. Dokumentami uzupełniającymi są załączniki, w odpowiedni sposób wymienione w polityce bezpieczeństwa.	
3.	Czy dokumentacja zarządzania systemem informatycznym reguluje zasady przetwarzania danych osobowych w zakresie: a) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności? b) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem?	Tak Tak		Przetwarzać dane może wyłącznie osoba posiadająca pisemne upoważnienie, nadane przez ADO. Stosowane metody i środki uwierzytelniania: konta użytkownika, identyfikator, hasło. Użytkownik zobowiązany jest do zmiany hasła minimum raz w miesiącu. Rozpoczęcie pracy odbywa się przez przygotowanie stanowiska pracy, włączeniu napięcia na listwie i włączenie stacji	

	c) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu? d) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania? e) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego? f) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych?	Tak Tak Tak Tak		roboczej, zalogowanie się do systemu, przy pomocy identyfikatora i hasła. Zawieszenie pracy jest możliwe po wylogowaniu z systemu informatycznego bądź zastosowaniu tzw. wygaszacza ekranu. Zakończenie pracy następuje poprzez wylogowanie się z aplikacji oraz systemu i następnie wyłączeniu wszystkich urządzeń, oraz zabezpieczeniu wszystkich dokumentów/nośników danych przed dostępem osób nieupoważnionych. Procedura tworzenia kopi zapasowych została szczegółowo opisana w dziale § 6 Instrukcji. Zastosowanie programów antywirusowych, zainstalowanie firewall, filtr antyspamowy, monitorowanie usług sieciowych, blokada dostępu do określonych stron, identyfikatory, indywidualne hasła, odpowiednia zmiana hasła. Procedura wykonywania przeglądów została opisana w § 10 Instrukcji.	
5.	Czy polityka bezpieczeństwa zawiera: a) zasady reagowania na incydent? b) obowiązki Inspektora Ochrony Danych? c) zasady raportowania z incydentu i ewidencjonowanie incydentów? d) zasady analizy incydentu?	Tak Tak Tak Tak		Każda osoba upoważniona do przetwarzania danych osobowych zobowiązań jest w razie zauważenia incydentu do niezwłocznego powiadomienia IOD, ASI lub ADO. IDO prowadzi postępowanie wyjaśniające w tym zakresie. Wszelkie ewentualne incydenty odnotowywane są w rejestrze przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych.	
6.	Ponadto czy dokumentacja zawiera: a) wymagania szkoleniowe? b) procedury kontrolne? c) procedury postępowania w przypadku naruszenia	Tak	Nie	Każda osoba zatrudniona w jednostce została przeszkolona a pracownikom nowo zatrudnianym przedstawiana jest dokumentacja oraz prezentacja	

	ochrony danych ? d) czy dokumentacja napisana jest językiem prostym i zrozumiałym dla wszystkich jej odbiorców?	Tak Tak		wykorzystana na szkoleniu. Procedury postępowania w przypadku naruszenia ochrony danych opisano w § 11 polityki. Dokumentacja jest napisana językiem prostym i zrozumiałym/	
7.	Czy dokumentacja przetwarzania danych osobowych zawiera także: a) decyzję/zarządzenie o wyznaczeniu Inspektora Ochrony Danych? b) upoważnienia do przetwarzania danych? c) ewidencję osób upoważnionych do przetwarzania danych? d) oświadczenia osób zapoznanych z dokumentacją oraz zobowiązanie do stosowania jej wymogów? e) listę osób przeszkolonych z zasad przetwarzania danych osobowych? f) oświadczenia pracowników o zachowaniu w tajemnicy danych osobowych? g) umowy o powierzeniu przetwarzania danych?	Tak Tak Tak Tak Tak TAK	Nie	IOD powołany został Zarządzeniem nr 35/2018 Wójta Gminy Goworowo z dnia 25.05.2018 r. Sprawdzono upoważnienia wszystkich pracowników. Ewidencja prowadzona jest w formie papierowej. W dokumentacji znajdują się oświadczenia wszystkich pracowników. W dniu 22.05.2018 r. zostali przeszkoleni wszyscy pracownicy urzędu, w aktach znajduje się stosowna lista. *Brak oświadczenia.* Umowa jest zawierana indywidualnie z każdym podmiotem.	
8.	Czy kierownictwo wspiera działania w zakresie bezpieczeństwa informacji w całej organizacji, w tym: a) w jaki sposób demonstrowane są cele, kierunki działania, zaangażowanie? (np. czy mówi się o tym na naradach, czy jest to temat powracający, na który kierownictwo zwraca uwagę?) b) jakie działania służą utrzymaniu właściwej świadomości problematyki bezpieczeństwa w organizacji? (np. kontrole, szkolenia) c) w jaki sposób przypisano role i zakresy odpowiedzialności za bezpieczeństwo informacji?	Tak		Wójt jak również IOD - w trakcie narad organizowanych z pracownikami omawia i analizuje działania związane z bezpieczeństwem informacji. Każdy pracownik, w tym nowo zatrudniony, obligatoryjnie zapoznaje się z dokumentacją dotyczącą polityki bezpieczeństwa. W Umowie o powołanie IOD wyszczególniono jego obowiązki.	

Tab. nr 2 Kwestionariusz samooceny – wypełniony przez informatyka zatrudnionego w Urzędzie Gminy pełniącego jednocześnie funkcję Administratora Systemu Informatycznego.

Nazwa zadania	***Bezpieczeństwo informacji***
Obiekt audytu	**Ochrona kluczowej infrastruktury i usług dla systemów IT – zabezpieczenia serwerowni**
Komórka audytowana	**ASI**

W kolumnie TAK / NIE proszę wstawić znak X

Lp.	Przedmiot zapytania (zagadnienie)	TAK	NIE	Uwagi / Informacje
1.	Drzwi antywłamaniowe		X	Drzwi wzmocnione blachą od wewnątrz
2.	Drzwi wyposażone w zamek atestowany		X	
3.	Samozamykacz		X	
4.	Elektroniczna kontrola dostępu		X	
5.	System przeciwpożarowy	X		Czujnik dymu podłączony do systemu przeciwpożarowego spiętego z systemem alarmowym dozoru budynku obsługiwanego przez zewnętrzną firmę ochroniarską (konsalnet)
6.	Zabezpieczenie przed zalaniem		X	
7.	System antywłamaniowy	X		System antywłamaniowy oparty na czujniku ruchu - kodowanych po zakończeniu pracy
8.	Klimatyzator	X		
9.	System gaszenia gazem		X	
10.	Okno w serwerowni Jeżeli jest okno to jak zabezpieczone:		X	Nie jest zabezpieczone.
10.1.	Krata zewnętrzna		X	
10.2.	Krata wewnętrzna		X	
10.3.	Roleta antywłamaniowa		X	
10.4.	Szyba antywłamaniowa		X	
10.5.	Folia antywłamaniowa		X	
10.6.	Inne – jakie?			
11.	Czy serwery mają zapewnione zasilanie awaryjne?	X		Każdy serwer podpięty jest pod centralny UPS

12.	Czy są przeprowadzane testy zasilania awaryjnego?	X		Kto? Jak często? Informatyk raz na kwartał
13.	Czy istnieją procedury przechowywania kluczy do serwerowni?		X	Czy pisemne? Klucz posiada tylko informatyk Drugi klucz jest przechowywany wraz z innymi kluczami w sekretariacie.
14.	Czy klucze przechowywane są w bezpiecznym miejscu?	X		W szafce zamykanej na klucz
15.	Czy istnieją procedury dotyczące wydawania i zdawania kluczy?	X		
16.	Czy istnieje rejestr pobierania i zdawania kluczy?	X		Klucze są wydawane zgodnie z rejestrem pobranych i zwróconych kluczy do pomieszczeń biurowych.
17.	Czy jest książka kontroli wejścia (rejestr kto, kiedy, w jakim celu wchodzi do serwerowni)	X		W serwerowni znajduje się rejestr pracy w pomieszczeniu serwerowni.
18.	Ile jest osób upoważnionych do wejścia?			Do wejścia do serwerowni upoważniony jest Sekretarz Gminy oraz informatyk. Inne osoby mogą wejść oraz przebywać w pomieszczeniu serwerowni tylko z ww. osobami.
19.	Czy w pomieszczeniu serwerowni są instalacje: c.o. i wod.-kan.?	X		Grzejnik CO,
20.	Czy istniej automatyczny system powiadamiania o przekroczeniu dopuszczalnej temperaturze?	X		Zamontowany jest czujniki jeden zewnętrzny a drugi w urządzeniu UPS, który powiadamia o o ewentualnym przekroczeniu temperatury dodatkowo powiadamia o zaniku zasilania.

Mając na uwadze powyższe wywody oraz ustalony stan faktyczny, Audytor Wewnętrzny stwierdza, że administrator danych (Wójt Gminy), który był odpowiedzialny za wdrożenie „właściwych" procedur oraz „odpowiednich" zabezpieczeń, w sposób stosunkowo pełny i prawidłowy wdrożył w jednostce procedury zawarte w rozporządzeniu RODO. Wdrożona zarządzeniem nr 42/2018 Wójta Gminy Goworowo z dnia 29.06.2018 r. dokumentacja (polityka ochrony danych osobowych oraz instrukcja zarządzania systemem informatycznym) spełnia wymagania stawiane przez obowiązujące przepisy prawa. Wdrożona dokumentacja przetwarzania danych osobowych jest instrumentem wykazującym zgodność wykonywanych czynności przetwarzania z przepisami prawa. Dokumentacja zawiera takie elementy jak:

1. rejestr czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;

2. wytyczne dotyczące procedury zgłaszania naruszenia ochrony danych do organu nadzorczego (UODO) – art. 33 ust 3 RODO;
3. procedurę na wypadek wystąpienia naruszeń mogących powodować wysokie ryzyko naruszenia praw i wolności osób, w zakresie ich informowania o działaniach, jakie powinni wykonać, aby ryzyko to ograniczyć – art. 34 RODO;
4. procedurę prowadzenia wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust 5 RODO;
5. raport z przeprowadzonej, ogólnej analizy ryzyka.

W odniesieniu do szeroko rozumianej dokumentacji przetwarzania danych osobowych jednostka sporządziła:

1. informacje udzielane osobom, których dane osobowe są przez jednostkę przetwarzane. Wzór takiej informacji został ustandaryzowany w wewnętrznej dokumentacji, co stanowi o ich prawidłowości i zgodności z przyjętym schematem;
2. klauzule zgód na przetwarzanie danych osobowych.

Wdrożona dokumentacja w zakresie przetwarzania danych osobowych, została opracowana zgodnie z podejściem opartym na szczegółowej analizie ryzyka. Efektem analizy ryzyka jest możliwość ustalenia, jakie należy wdrożyć środki, które pozwolą na zmniejszenie ustalonego ryzyka, a tym samym – zwiększenie poziomu zabezpieczeń danych osobowych. Całość opisanych powyżej działań, podjętych przez Administratora, pozwala na minimalizację ryzyka związanego z przetwarzaniem danych osobowych. Zaznaczyć nadto należy, że wszyscy pracownicy zapoznali się z nową dokumentacją, oraz przeszli obowiązkowe szkolenie w tym zakresie. Jednostka powołała również Inspektora Ochrony Danych Osobowych.

Dodatkowo audytor zaleca wprowadzenia do już stosowanego w jednostce oświadczenia stanowiącego załącznik nr 2 do Polityki ochrony danych zapisu o zachowaniu w tajemnicy przetwarzanych danych osobowych.

Podsumowując: Audytor wewnętrzny, realizując zadanie zapewniające nie stwierdza żadnych istotnych uchybień - system kontroli zarządczej w badanym zakresie funkcjonuje w jednostce na poziomie prawidłowym. Nie zauważono podwyższonego ryzyka mogącego stanowić zagrożenie dla realizacji celów stawianych przed systemem bezpieczeństwa informacji. Wdrożona przez jednostkę dokumentacja w zakresie bezpieczeństwa informacji jest kompleksowa i aktualna, oraz spełnia wymogi wynikające z przepisów prawa, w tym stawiane przez RODO.

Jednocześnie zauważyć należy, iż w związku z brakiem zabezpieczenia okna, które znajduje się w pomieszczeniu serwerowni, audytor zaleca podjęcie działań w celu jego zabezpieczenia czy to przez zastosowanie foli antywłamaniowej czy też za pomocą rolety zewnętrznej. Z uwagi, iż pomieszczenie serwerowni zlokalizowane jest na I piętrze budynku Urzędu jak również wyposażone jest w czujnik sygnalizujący włamanie zastosowanie folii antywłamaniowej wydaje się rozwiązaniem, które zapewni zabezpieczenie, w sposób wystarczający aczkolwiek kwestia wyboru rodzaju zabezpieczenia winna zostać przeanalizowana i wybrana przez Kierującego Urzędem.

Zgodnie z § 17 ust. 1 rozporządzenia Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu[7] audytor wewnętrzny po przeprowadzeniu czynności audytowych omawia z audytowanym wstępne wyniki audytu, w tym w szczególności ustalenia i propozycje zaleceń. Realizując dyspozycję tego przepisu audytor wewnętrzny w dniu 4.04.2020 r. przekazał audytowanemu drogą elektroniczną projekt sprawozdania, zawierający ustalenia oraz – ewentualnie - propozycje zaleceń. W dniu 8.04.2020 r. audytowany zaakceptował sprawozdanie.

Z kolei § 19 ust. 1 tego rozporządzenia mówi, że kierownik komórki audytu wewnętrznego przekazuje sprawozdanie audytowanemu i kierownikowi jednostki; w przypadku odmowy realizacji zaleceń audytowany przedstawia, w terminie 7 dni kalendarzowych od dnia otrzymania sprawozdania, pisemne stanowisko kierownikowi jednostki i audytorowi wewnętrznemu (ust. 3).

Sprawozdanie to sporządzono w dwóch jednobrzmiących egzemplarzach, które otrzymują:

1. Wójt Gminy Goworowo,
2. a/a.

Audytor wewnętrzny

.....Marek Żuczek.....

(podpis audytora)

[7] Rozporządzenie Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu, Dz. U. z 2015 r. poz. 1480 ze zm.