Urząd Miejski Gołdap	
Program zadania zapewniającego - audytowego	
Temat zadania:	Dostosowanie Urzędu Miejskiego w Gołdapi do wymogów ogólnego rozporządzenia o ochronie danych (RODO)/KRI
Cel zadania:	Zadanie zapewniające dot. stopnia wdrożenia systemu ochrony danych osobowych zgodnych z Rozporządzeniem RODO oraz wymogów dot. zarządzania bezpieczeństwem systemów informatycznych/KRI
Zakres podmiotowy i przedmiotowy zadania:	Zakres przedmiotowy – obszar wdrożenia regulacji dot. ochrony danych osobowych (zgodnie z Rozporządzeniem RODO) oraz zarządzania bezpieczeństwem systemów IT zgodnie z Rozporządzeniem KRI. Zakres podmiotowy – Urząd Miejski w Gołdapi, Inspektor Ochrony Danych, Administrator Systemów Informatycznych.
Istotne ryzyka w obszarze działalności jednostki objętym zadaniem:	• Brak dostosowania obszaru ochrony danych osobowych do wymogów RODO, • Brak powołania IOD, • Brak dostosowania działań Urzędu i realizowanych zadań publicznych do wymogów KRI,
Sposób zrealizowania zadania, w szczególności opis doboru próby do badania oraz technik badania:	Wywiady z osobami odpowiedzialnymi za funkcjonowanie obszarów, badanie dokumentacji, obserwacja.
Uzgodnione kryteria oceny:	• zgodność z przepisami prawa i regulacjami wewnętrznymi w zakresie wskazanym w treści załączników do Programu: - załącznik nr 1 Ocena RODO - załącznik nr 2 Systemy Informatyczne/KRI
Data rozpoczęcia i zakończenia zadania:	Rozpoczęcie: 7 marca 2019 r. Zakończenie: 30 czerwca 2019 r.
Audytor:	Adrian Chodubski, CGAP, MF

Warszawa, 7 marca 2019 r.

uzgodniono!
BURMISTRZ
GOŁDAPI
Tomasz Luto

Adrian Chodubski
Audytor wewnętrzny
CGAP nr. IAIS MF 1709/2018

Aesco Group

ul. Sienna 72A/1602
00-833 Warszawa

22 213 81 60
22 213 81 66

biuro@aesco.com.pl

Warszawa, 11 czerwca 2019 r.

Urząd Miejski w Gołdapi
WPŁYNĘŁO
11. 06. 2019
Nr rej. ..... zał. .....
Skier. ..... podpis .....

Szanowna Pani
Anna Rawinis
Sekretarz
Gminy Gołdap
<anna.rawinis@goldap.pl>

Szanowna Pani Sekretarz,

w nawiązaniu do zrealizowanego zadania audytowego pn. „Dostosowanie Urzędu Miejskiego w Gołdapi do wymogów ogólnego rozporządzenia o ochronie danych (RODO) oraz do wymogów KRI za okres od 2018 r. do dnia audytu" przedkładam sprawozdanie wstępne z zadania audytowego.

Proszę o zgłoszenie ewentualnych uwag do treści sprawozdania do dnia 19 czerwca br. Ewentualne uwagi proszę przesłać na adres adrian.chodubski@aesco.com.pl.

W razie pytań pozostaję w kontakcie mailowym i telefonicznym.

Łączę wyrazy szacunku

Adrian Chodubski
Audytor wewnętrzny
CIAP no. UIE MP 1700/2015

Uwagi do sprawozdania wstępnego w dniu 19.06.2018 r.
Sekretarz Gminy Gołdap
mgr Anna Rawinis

Adrian Chodubski
Główny Specjalista ds. Audytu Wewnętrznego JST

tel. kom. (+48) 792 008 131
adrian.chodubski@aesco.com.pl
www.aesco.com.pl

Aesco Group

Aesco Group Sp. z o.o.
ul. Sienna 72a/1602
00-833 Warszawa
Tel. (+48) 22 213 81 60
Fax (+48) 22 213 81 66
biuro@aesco.com.pl

Sprawozdanie z audytu nr 1/2019 w zakresie dostosowanie Urzędu Miejskiego w Gołdapi do wymogów ogólnego rozporządzenia o ochronie danych (RODO) oraz do wymogów KRI

Termin audytu:	14.03.2019 r. i 09.04.2019 r.
Data sprawozdania:	11.06.2019 r.

Audytor:	Adrian Chodubski CGAP, MF

Wstęp

Tematem zadania zapewniającego była ocena „dostosowanie Urzędu Miejskiego w Gołdapi do wymogów ogólnego rozporządzenia o ochronie danych (RODO) oraz do wymogów KRI za okres od 2018 r. do dnia audytu". Zadanie audytowe zostało przeprowadzone zgodnie z rocznym planem pracy na rok 2019 – poz. 1, na podstawie Umowy zawartej pomiędzy Gminą Gołdap, a Aesco Group Sp. z o.o. W ramach czynności audytowych przeprowadzono wizytę audytową w dniach 14 marca 2019 r. oraz 9 kwietnia 2019 r. Audyt przeprowadził Adrian Chodubski, CGAP no. 1318 MF 1700/2005 – audytor spełniający wymogi o których mowa w art. 286 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

Celem działań było przeprowadzenie audytu dot. oceny dostosowania rozwiązań w obszarze ochrony danych osobowych do wymogów przepisów RODO oraz wymogów KRI na poziomie Urzędu Miejskiego w Gołdapi (dalej: „Urząd"). Zadanie audytowe przeprowadzone zostało w oparciu o program zadania z dnia 14 marca 2019 r. W ramach czynności audytowych przeprowadzono:

- analizę dokumentów organizacyjnych dot. funkcjonowania obszaru danych osobowych Urzędu oraz obszaru IT,
- analizę wybranych dokumentów Urzędu,
- porównanie informacji z różnych źródeł,
- wywiad z Inspektorem ochrony danych p. Sebastianem Liwak oraz Administratorem Systemów Informatycznych – p. Piotrem Mietlińskim.

Ustalenia z audytu

Weryfikacji stanu faktycznego dokonano w oparciu o zgodność z zapisami:

- Rozporządzenia 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) (L 119/1 z dnia 4.5.2016) – (dalej: „Rozporządzenie RODO"),

- ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000 ze zm.),
- Obwieszczenie Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. poz. 2247) - (dalej: „KRI"),
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64 poz. 565 ze zm.).

W wyniku przeprowadzonych czynności stwierdzono, iż regulacje w zakresie ochrony danych osobowych wdrożono Zarządzeniem Nr 123/II/2019 Burmistrza Gołdapi z dnia 19 lutego 2019 r. w sprawie wprowadzenia "Polityki Ochrony Danych Osobowych" w Urzędzie Miejskim w Gołdapi (dalej: „Polityka").

Stwierdzono, iż funkcję Inspektora ochrony danych powierzono pracownikowi p. Sebastianowi Liwak[1] (dalej: „Inspektor" lub „IOD"). W wyniku analizy dokumentacji stwierdzono, iż Inspektor legitymuje się doświadczeniem w obszarze ochrony danych osobowych, dającym gwarancję poprawności realizacji zadań wynikających z pełnionej funkcji. W wyniku analizy zapisów regulaminu organizacyjnego Urzędu stwierdzono, iż treści regulacji brak jest zdefiniowanych zadań Inspektora oraz brak jest określonych zasad współpracy komórek organizacyjnych Urzędu z IOD[2].

W ocenie audytora należy rozważyć dokonanie aktualizacji zapisów regulaminu organizacyjnego Urzędu, poprzez wprowadzenie do treści regulacji funkcji Inspektora oraz zasad współpracy komórek organizacyjnych z IOD. Rekomendacja ma charakter fakultatywny.

Na poziomie Urzędu przeprowadzono przez Inspektora w dniach 16-18 października 2018 r. szkolenie w zakresie nowych przepisów ochrony danych osobowych. Stwierdzono,

1 Umowa na świadczenie usług związanych z realizacją zadań przypisanych inspektorowi Ochrony danych w Urzędzie Miejskim w Gołdapi z dnia 31.12.2018 r. Zarządzenie Nr 1379/VII/2018 Burmistrza Gołdapi z dnia 26 lipca 2018 r. w sprawie wyznaczenie Inspektora Ochrony Danych w Urzędzie Miejskim w Gołdapi.
2 Zarządzenie Nr 883/II/2014 Burmistrza Gołdapi z dnia 27 lutego 2014 r. w sprawie nadania Regulaminu Organizacyjnego Urzędowi Miejskiemu w Gołdapi ze zm.

iż Administrator dokumentuje proces upoważniania do przetwarzania danych osobowych w sposób, który umożliwia ustalenie wszystkich osób zaangażowanych w procesy przetwarzania danych na poziomie Urzędu. Wszystkie podmioty przetwarzające dane osobowe (w tym inne podmioty przetwarzające, które wykonują usługi na ich rzecz) zostały upoważnione przez Administratora, a przetwarzanie danych zostało powierzone w formie pisemnej. Na poziomie Urzędu dokonano inwentaryzacji umów powierzenia danych osobowych. Wypracowane w jednostce wzory umów albo klauzul umownych związanych ze świadczeniem usług przetwarzania danych osobowych są prawidłowe.

Dla wszystkich zbiorów danych/procesów przetwarzania danych zidentyfikowano podstawę prawną oraz warunki ich przetwarzania. Czynności zrealizowane przez Administratora zostały udokumentowane w rejestrze czynności przetwarzania danych osobowych. Urząd dokonał identyfikacji określonych w prawie celów przetwarzania danych osobowych.

Stwierdzono, iż na poziomie Urzędu nie dokonano identyfikacji danych osobowych, dla których podstawą przetwarzania jest zgoda. Ponadto w ocenie audytora w Urzędzie nie funkcjonuje system rejestrowania i zarządzania bieżącą zgodą na przetwarzanie danych osobowych. W treści Polityki nie określono w zasad przetwarzania danych osobowych dla których podstawą ich przetwarzania jest zgoda osoby fizycznej.

W ocenie audytora, w terminie do dnia 31 grudnia 2019 r., należy dokonać aktualizacji zapisów Polityki poprzez wprowadzenie zapisów dot. systemu rejestrowania i zarządzania bieżącą zgodą na przetwarzanie danych osobowych.

Na poziomie Urzędu opracowano procedurę udzielania informacji osobom, których dotyczą dane osobowe. Ponadto opracowano treść klauzuli informacyjnej dla osób, od których dane osobowe będą pozyskiwane. Treść opracowanych klauzul informacyjnych spełnia wymogi Rozporządzenia RODO. Urząd określił procedury postepowania w obszarze realizacji praw osoby, której dane dotyczą, a w szczególności w obszarze prawa dostępu do danych osobowych, sprostowania i usuwania danych osobowych, ograniczenia dostępu do danych osobowych oraz przenoszenia danych osobowych.

Stwierdzono, iż w Urzędzie funkcjonuje rejestr osób, którym nadano uprawnienia do przetwarzania danych osobowych. Rejestr obejmuje dane pracowników Urzędu oraz pracowników okresowych (stażyści i praktykanci). W rejestrze odnotowywane są zdarzenia

nadające uprawnienia do przetwarzania danych pracownikom Urzędu, jak również zdarzenia dotyczące wygaśnięcia/cofnięcia uprawnień do przetwarzania danych. Proces nadawania i cofania uprawnień jest należycie udokumentowany. Z treści upoważnienia wynika zakres dostępu do kategorii/zbiorów danych, jak również czy dane przetwarzane są w formie manualnej papierowej czy elektronicznej (w uzasadnionych przypadkach jest wskazany system lub oprogramowanie).

Urząd prowadzi ewidencję podmiotów przetwarzających dane osobowe w imieniu Administratora. Powierzenie realizacji zadań nastąpiło w formie pisemnej. Stwierdzono, iż jednostka opracowała wzór umowy powierzenia danych. Wzór dokumentu zawiera elementy wskazane w art. 28 Rozporządzenia RODO. Urząd dla wszystkich zbiorów danych/procesów przetwarzania danych zidentyfikował podstawę prawną (warunki przetwarzania). Informacja ta została zawarta w rejestrze czynności przetwarzania.

W rejestrze określono:

- czynność przetwarzania,
- cele przetwarzania,
- planowane terminy usunięcia poszczególnych kategorii danych,
- opis środków technicznych i organizacyjnych,
- kategorie osób których dane dotyczą,
- kategorie osób którym dane zostaną przekazane,
- przekazanie danych do państwa trzeciego.

Administrator wyznaczył osoby właściwe w zakresie zgłaszania Prezesowi UODO naruszeń ochrony danych osobowych, które skutkują ryzykiem naruszenia praw lub wolności osób fizycznych. Urząd opracował właściwą procedurę zgłaszania i postępowania z naruszeniami ochrony danych osobowych. Na poziomie Urzędu prowadzony jest rejestr naruszeń ochrony danych osobowych, który dokumentuje w szczególności wszystkie przypadki zgłoszeń, w tym tych, które nie podlegają obowiązkowi przekazania do Prezesowi UODO.

Stwierdzono, iż na poziomie Urzędu nie dokonano identyfikacji operacji przetwarzania danych, dla których poziom ryzyka naruszenia praw lub wolności osób fizycznych oceniono, jako wysoki.

W ocenie audytora należy, w terminie do dnia 31 grudnia 2019 r., dokonać oceny skutków dla ochrony danych, zawierającej elementy określone w treści art. 35 ust. 7 Rozporządzenia RODO, tj:,

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym (gdy ma to zastosowanie) prawnie uzasadnionych interesów realizowanych przez Administratora,
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych.

Urząd opracował i ustanowił, wdrożył oraz eksploatuje, monitoruje i przegląda, utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Kompleksowa dokumentacja systemu zarządzania bezpieczeństwem informacji określona została w treści Zarządzeniem Nr 123/II/2019 Burmistrza Gołdapi z dnia 19 lutego 2019 r. w sprawie wprowadzenia "Polityki Ochrony Danych Osobowych" w Urzędzie Miejskim w Gołdapi.

Urząd posiada skrzynkę e-PUAP skonfigurowaną z systemem COIK. Wszystkie dokumenty wchodzące na skrzynkę podawczą przekazywane są do realizacji właściwych komórek organizacyjnych za pośrednictwem systemu IntraDOK. Urząd nie wykorzystuje wzorów dokumentów elektronicznych przechowywanych w Centralnym Repozytorium Wzorów Dokumentów Elektronicznych, jakie zostały już wcześniej opracowane i są używane przez inne podmioty publiczne. Jednocześnie Urząd nie przekazywał do Repozytorium wzorów dokumentów elektronicznych podmiotu publicznego.

Urząd właściwie zarządza usługami elektronicznymi w oparciu o model usługowy. Na poziomie Urzędu funkcjonuje produkt opracowany w ramach projektu „Cyfrowe usługi w zakresie udostępniania informacji publicznej Urzędu Miejskiego w Gołdapi" dofinansowanego w ramach środków Europejskiego Funduszu Rozwoju Regionalnego w ramach RPO Warmińsko-Mazurskiego 2014-2020. Zasady eksploatacji systemu, określone w dokumentacji powykonawczej z dnia 20 sierpnia 2018 r., wykorzystują model usługowy w procesie świadczenia usług elektronicznych. Pełne wdrożenie rezultatów projektu zakłada implementację usług w systemie Katalogu e- Usług, obejmujących:

- udostępnienie danych z Rejestru Dowodów Osobistych oraz dokumentacji związanej z dowodami osobistymi. Wydanie zaświadczenia z dokumentacji związanej z dowodami osobistymi,
- uzgodnienie dokumentacji technicznej i dysponowanie gruntem na cele budowlane,
- uzgodnienie lokalizacji zjazdu w pasie drogowym,
- uzgodnienie lokalizacji obiektów budowlanych lub urządzeń infrastruktury technicznej niezwiązanej z potrzebami zarządzania drogami lub potrzebami ruchu drogowego,
- wydanie zezwolenia na zajęcie pasa drogowego drogi w celu prowadzenia robót związanych z budowa lub przebudowa zjazdu,
- interwencje dot. stanów technicznych, remontów lokali i budynków stanowiących mieszkaniowy zasób gminy (miasta),
- przydział lokalu mieszkalnego,
- wydanie odpisu z rejestru stanu cywilnego,
- wniosek o wykonanie przewozów na liniach komunikacyjnych na obszarze gminy,
- wniosek o udzielnie licencji w zakresie przewozu osób i pośrednictwa,
- wniosek o nadanie awansu zawodowego nauczyciela mianowanego,
- wniosek o przyznanie pomocy materialnej o charakterze socjalnym lub zasiłku szkolnego,
- wpis do ewidencji obiektów, w których świadczone są usługi hotelarskie,
- wniosek o objęcie przedsięwzięcia patronatem honorowym Burmistrza,
- wniosek o wyrażenie zgody na używanie herbu miasta,
- wniosek o uzyskanie dotacji w ramach programu współpracy,
- zawiadomieni o zaprzestaniu wykonywania działalności gospodarczej,
- zezwolenie na sprzedaż napojów alkoholowych,
- wniosek o wydanie decyzji na zorganizowanie imprezy masowej.

Na poziomie Urzędu wykorzystywane jest system zarządzania dokumentami elektronicznymi, wpływający na uporządkowanie i usprawnienie przepływu dokumentów w Urzędzie[3]. System IntraDok firmy COIG S.A. wdrożony został w jednostce w ramach

3 Zarządzenie Nr 1007/VII/2017 Burmistrza Gołdapi z dnia 31 lipca 2017 r. w sprawie wskazania systemu wykonania czynności kancelaryjnych, wyznaczenia koordynatora czynności kancelaryjnych oraz określenia rodzaju przesyłek wpływających, które nie są otwierane przez punkt kancelaryjny w UM w Gołdapi

projektu współfinansowanego ze środków RPO Warmińsko-Mazurskiego 2014-2020. Wdrożone narzędzie ma charakter wspomagający do tradycyjnego systemu obiegu dokumentów funkcjonującego w Urzędzie. Na dzień audytu system współpracuje z e- PUAP i docelowo będzie współpracował z modelem e-Usługi.

Urząd współdzieli informacje w sposób umożliwiający wymianę danych pomiędzy różnymi systemami informatycznymi oraz umożliwia odbiorcom swobodny dostępu do informacji, poprzez wygenerowanie danych w powszechnie znanych i dostępnych formatach plików. Urząd nie dysponuje wykazem formatów danych wykorzystywanych na poziomie systemów informatycznych Urzędu. Dokumentacja systemu IntraDok nie zawiera wykazu obsługiwanych przez system informatycznych danych. Nie stwierdzono przypadków braku możliwości przetwarzania danych przez system Intra Dok.

Stwierdzono, iż na poziomie Urzędu nie przeprowadzono okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, obejmującej następujące elementy:

- identyfikacja ryzyka (wpływ zagrożeń na podatności),
- analiza ryzyka w tym określenie poziomu ryzyka (kombinacja prawdopodobieństwa wystąpienia i skutków/następstw),
- ocena ryzyka (porównywanie poziomu ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane),
- określenie sposobu postępowania z ryzykiem (dla ryzyka, którego wielkość jest nieakceptowalna).

Na poziomie Urzędu nie opracowano dokumentu zawierającego wyniku procesu zarządzania ryzykiem, przedstawiającego plan postępowania z ryzykiem utraty integralności, dostępności lub poufności informacji.

W ocenie audytora, w terminie do dnia 31 grudnia 2019 r., należy przeprowadzić kompleksową analizę ryzyka utraty integralności, dostępności lub poufności informacji. Proces identyfikacji, analizy i oceny ryzyka powinien być powiązany z oceną ryzyka oceny skutków dla ochrony danych, zawierającej elementy określone w treści art. 35 ust. 7 Rozporządzenia RODO.

Urząd posiada aktualny stan inwentarzowy sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Procedura ewidencjonowania urządzeń i nośników informacji zdefiniowana została w załączniku B2 do Polityki. Zgodnie

z regulacją w Urzędzie prowadzony jest rejestr urządzeń i nośników służących do przetwarzania danych osobowych. Obecnie w fazie opracowywania przez ASI jest nowe narzędzie ewidencyjne na bazie programu MS Excel.

W ocenie audytora należy rozważyć wykorzystanie ogólnodostępnego oraz darmowego oprogramowania typu „open source" umożliwiającego ewidencjonowanie urządzeń i nośników informacji. Audytor rekomenduje wykorzystanie narzędzia producent GLPI[4].

Urząd właściwie zarządza dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem zapewnia, 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, a w przypadku zmiany zadań następuje również zmiana ich uprawnień. Nie stwierdzono sytuacji, aby uprawnienia administratora wszystkich kluczowych zasobów IT posiadała jedna osoba.

Stwierdzono, iż zapisy Polityki wskazują, iż w Urzędzie uprawnione do przetwarzania danych osobowych są wyłącznie osoby upoważnione do wykonywania tych czynności. Administrator jest uprawniony do przyznawania indywidualnych upoważnień w przedmiocie przetwarzania danych osobowych. W dokumentacji w obszarze upoważnień do przetwarzania danych osobowych określono, iż nowozatrudnieni pracownicy UM, po nadaniu upoważnienia do przetwarzania danych osobowych, uczestniczą w szkoleniu prowadzonym przez IOD, mającym na celu zaznajomienie użytkownika z obowiązującymi przepisami prawa, z wewnętrzną dokumentacją obowiązującą w jednostce.

Urząd zapewnia podnoszenie świadomości zagrożeń i konsekwencji zaistnienia incydentów związanych z naruszeniem bezpieczeństwa informacji pracowników. Na poziomie Urzędu Miejskiego w Gołdapi szkoleniem z zakresu ochrony danych osobowych objęto pracowników jednostki w dniach 16-18.10.2018 r. W dokumentacji w obszarze upoważnień do przetwarzania danych osobowych określono, iż nowozatrudnieni pracownicy Urzędu, po nadaniu upoważnienia do przetwarzania danych osobowych, uczestniczą w szkoleniu prowadzonym przez IOD, mającym na celu zaznajomienie użytkownika z obowiązującymi przepisami prawa, z wewnętrzną dokumentacją obowiązującą w jednostce.

Urząd wprowadził regulacje wewnętrzne zawierające zasady bezpiecznej pracy użytkowników, przy wykorzystaniu urządzeń przenośnych i pracy na odległość. Zasady

4 https://glpi-project.org/

korzystania z komputerów przenośnych określone zostały w procedurze korzystania z komputera służbowego (załącznik B.4 Polityki). Określono zasady zabezpieczenia komputera przenośnego w czasie transportu. W procedurze wskazano zakaz logowania się do otwartych sieci (hotspoty, otwarte Wi-Fi).

Urząd zapewnił objęcie systemów informatycznych o znaczeniu krytycznym stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych). Umowy serwisowe posiadają klauzule prawne zabezpieczające bezpieczeństwo informacji, w przypadku wejścia w ich posiadanie przez podmioty zewnętrzne.

Stwierdzono, iż w regulacjach wewnętrznych Urzędu nie określono zasad zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji oraz ewentualnych zasad współpracy z cert.gov.pl, zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI.

W ocenie audytora, w terminie do dnia 31 grudnia 2019 r., należy dokonać opracowania i wdrożenia regulacji definiujących zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji oraz ewentualnych zasad współpracy z cert.gov.pl.

Urząd zapewnia wykonywanie kopii zapasowych umożliwiających odzyskanie danych i przywrócenie do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system. Urząd wykonuje regularnie kopie zapasowe całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych. Ponadto wykonywane są regularne testy jakości kopii zapasowych, poprzez odtworzenie systemu informatycznego z kopii zwykle na niezależnym od środowiska produkcyjnego sprzętowym środowisku testowym oraz testowaniu pracy użytkowej odtworzonego systemu.

Urząd właściwie zabezpiecza informacje w sposób uniemożliwiający nieuprawnionemu ich ujawnieniu, modyfikacji, usunięciu lub zniszczeniu. Ponadto Urząd zapewnia aby w dziennikach systemów zostały odnotowane obligatoryjnie działania użytkowników lub obiektów systemowych. Urząd zapewnia ochronę przetwarzanych informacji przed ich

kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. W poddanych weryfikacji regulacjach wewnętrznych stwierdzono, iż ustalono w nich zasady zapewniające:

- minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, oraz urządzeń mobilnych,
- ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, poprzez ustalenie zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie,
- monitorowanie dostępu do informacji,
- możliwość wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, poprzez kontrolę logów systemów, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę rejestru zgłoszeń serwisowych, analizę rejestru incydentów naruszenia bezpieczeństwa informacji,
- środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji, poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowanie systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall,
- działania związane z utylizacją sprzętu informatycznego i nośników danych a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie bezpieczeństwa informacji.

Stwierdzono, iż w systemach teleinformatycznych stosowane są zabezpieczenia techniczno-organizacyjne dotyczące środowiska teleinformatycznego pracy danego systemu.

ASI podejmuje działania związane z aktualizacją oprogramowania oraz redukcją ryzyka wynikającego z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych, poprzez wdrażanie nowych wersji oprogramowania systemowego i użytkowego, poprawek i uzupełnień podnoszących ich bezpieczeństwo, aktualizację oprogramowania antywirusowego i antyspamowego, aktualizację oprogramowania zabezpieczającego ruch sieciowy, itp. Ponadto podejmowane są działania obejmujące minimalizowanie ryzyka utraty informacji w wyniku awarii oraz ochrony przed błędami, utratą i nieuprawnioną modyfikacją, a także zapewnieniem bezpieczeństwa plików systemowych, poprzez zastosowanie bezpiecznych i redundantnych rozwiązań sprzętowych,

w tym: dwustronnego bezprzerwowego zasilania, redundancji klimatyzacji, zastosowania klastra serwerów wysokiej dostępności, redundancji macierzy dyskowych i urządzeń sieciowych, równoważenie obciążenia, monitorowanie parametrów środowiskowych w serwerowni (temperatura, wilgotność, zadymienie, wyciek wody), zastosowanie systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci.

Urząd zapewnił przetwarzanie informacji w systemach teleinformatycznych z wymogiem dostępu do danych przez uprawnione osoby i obiekty systemowe (procesy), w ustalonym zakresie. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i co wykonał w systemie teleinformatycznym. Wykonywane czynności obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi).

Stwierdzono, iż Urząd uwzględnia potrzeby osób niepełnosprawnych poprzez stosowanie w eksploatowanych systemach teleinformatycznych rozwiązań technicznych umożliwiających osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. W systemie teleinformatycznym Urzędu zapewniono spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do Rozporządzenia KRI. Zastosowane narzędzia uwzględniają rozwiązania techniczne, umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu.

Podsumowanie

Na podstawie przeprowadzonych czynności audytowych audytor wydaje ocenę pozytywną nt. funkcjonowania obszaru ochrony danych osobowych oraz spełniania wymogów KRI na poziomie Urzędu Miejskiego w Gołdapi.

Stosowane w ramach audytowanego obszaru mechanizmy kontrolne skutecznie minimalizują możliwość materializacji zagrożeń mogących mieć istotny, negatywny wpływ na realizację celów i zadań w obszarze objętym zadaniem audytowym.

W audytowanym obszarze funkcjonuje adekwatny, skuteczny i efektywny system kontroli zarządczej, z zastrzeżeniami wskazanymi w treści sprawozdania.

Zalecenia i rekomendacje

Lp.	Treść	Termin	Ryzyko
1*	Należy rozważyć dokonanie aktualizacji zapisów regulaminu organizacyjnego Urzędu, poprzez wprowadzenie do treści regulacji funkcji Inspektora oraz zasad współpracy komórek organizacyjnych z IOD.	----	Ryzyko o charakterze niskim (💣)
2	Należy dokonać aktualizacji zapisów Polityki Ochrony Danych Osobowych, poprzez wprowadzenie zapisów dot. systemu rejestrowania i zarządzania bieżącą zgodą na przetwarzanie danych osobowych.	31 grudnia 2019	Ryzyko o charakterze średnim (💣 💣))
3	Należy dokonać oceny skutków dla ochrony danych, zawierającej elementy określone w treści art. 35 ust. 7 Rozporządzenia RODO, tj:, - systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym (gdy ma to zastosowanie) prawnie uzasadnionych interesów realizowanych przez Administratora, - ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów, - ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, - środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające	31 grudnia 2019	Ryzyko o charakterze średnim (💣 💣)

	zapewnić ochronę danych osobowych.		
4	Należy przeprowadzić kompleksową analizę ryzyka utraty integralności, dostępności lub poufności informacji. Proces identyfikacji, analizy i oceny ryzyka powinien być powiązany z oceną ryzyka oceny skutków dla ochrony danych, zawierającej elementy określone w treści art. 35 ust. 7 Rozporządzenia RODO.	31 grudnia 2019	Ryzyko o charakterze średnim (💣💣)
5*	Należy rozważyć wykorzystanie ogólnodostępnego oraz darmowego oprogramowania typu „open source" umożliwiającego ewidencjonowanie urządzeń i nośników informacji. Audytor rekomenduje wykorzystanie narzędzia producent GLPI	----	Ryzyko o charakterze niskim (💣)
6	Należy dokonać opracowania i wdrożenia regulacji definiujących zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji oraz ewentualnych zasad współpracy z cert.gov.pl.	31 grudnia 2019	Ryzyko o charakterze średnim (💣💣)
Skala ryzyka: 💣 niskie, 💣💣 średnie, 💣💣💣 wysokie, N krytyczne			

* - rekomendacja ma charakter fakultatywny. Decyzja o wdrożeniu rekomendacji należy do kierownika jednostki audytowanej.

Adrian Chodubski
Audytor wewnętrzny
CIAP nr: [illegible] MF 1209/2015

Zapoznałem się ze sprawozdaniem:
Burmistrz Gminy Gołdap (data i podpis)

Aesco Group

ul. Sienna 72A/1602
00-833 Warszawa

22 213 81 60
22 213 81 66

biuro@aesco.com.pl

Warszawa, 28 czerwca 2019 r.

Szanowna Pani
Anna Rawinis
Sekretarz
Gminy Gołdap
<anna.rawinis@goldap.pl>

Szanowna Pani Sekretarz,

w nawiązaniu do zrealizowanego zadania audytowego pn. „Dostosowanie Urzędu Miejskiego w Gołdapi do wymogów ogólnego rozporządzenia o ochronie danych (RODO) oraz do wymogów KRI za okres od 2018 r. do dnia audytu" przedkładam sprawozdanie z zadania audytowego.

Zgłoszone przez Państwa ustne uwagi do wstępnej wersji sprawozdania zostały w całości uwzględnione. Wprowadzono stosowne zmiany w treści sprawozdania.

W razie pytań pozostaję w kontakcie mailowym i telefonicznym.

Łączę wyrazy szacunku

Adrian Chodubski
Audytor wewnętrzny
CIA nr. EIIR MP 1700/2015

Adrian Chodubski
Główny Specjalista ds. Audytu Wewnętrznego JST

tel. kom. (+48) 792 008 131
adrian.chodubski@aesco.com.pl
www.aesco.com.pl

Aesco Group

Aesco Group Sp. z o.o.
ul. Sienna 72a/1602
00-833 Warszawa
Tel. (+48) 22 213 81 60
Fax (+48) 22 213 81 66
biuro@aesco.com.pl

Sprawozdanie z audytu nr 1/2019 w zakresie dostosowanie Urzędu Miejskiego w Gołdapi do wymogów ogólnego rozporządzenia o ochronie danych (RODO) oraz do wymogów KRI

Termin audytu:	14.03.2019 r. i 09.04.2019 r.
Data sprawozdania:	28.06.2019 r.
Audytor:	Adrian Chodubski CGAP, MF

Wstęp

Tematem zadania zapewniającego była ocena „dostosowanie Urzędu Miejskiego w Gołdapi do wymogów ogólnego rozporządzenia o ochronie danych (RODO) oraz do wymogów KRI za okres od 2018 r. do dnia audytu". Zadanie audytowe zostało przeprowadzone zgodnie z rocznym planem pracy na rok 2019 – poz. 1, na podstawie Umowy zawartej pomiędzy Gminą Gołdap, a Aesco Group Sp. z o.o. W ramach czynności audytowych przeprowadzono wizytę audytową w dniach 14 marca 2019 r. oraz 9 kwietnia 2019 r. Audyt przeprowadził Adrian Chodubski, CGAP no. 1318 MF 1700/2005 – audytor spełniający wymogi o których mowa w art. 286 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

Celem działań było przeprowadzenie audytu dot. oceny dostosowania rozwiązań w obszarze ochrony danych osobowych do wymogów przepisów RODO oraz wymogów KRI na poziomie Urzędu Miejskiego w Gołdapi (dalej: „Urząd"). Zadanie audytowe przeprowadzone zostało w oparciu o program zadania z dnia 14 marca 2019 r. W ramach czynności audytowych przeprowadzono:

- analizę dokumentów organizacyjnych dot. funkcjonowania obszaru danych osobowych Urzędu oraz obszaru IT,
- analizę wybranych dokumentów Urzędu,
- porównanie informacji z różnych źródeł,
- wywiad z Inspektorem ochrony danych p. Sebastianem Liwak oraz Administratorem Systemów Informatycznych – p. Piotrem Mietlińskim.

Ustalenia z audytu

Weryfikacji stanu faktycznego dokonano w oparciu o zgodność z zapisami:

- Rozporządzenia 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) (L 119/1 z dnia 4.5.2016) – (dalej: „Rozporządzenie RODO"),
- ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000 ze zm.),

- Obwieszczenie Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. poz. 2247) - (dalej: „KRI"),
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64 poz. 565 ze zm.).

W wyniku przeprowadzonych czynności stwierdzono, iż regulacje w zakresie ochrony danych osobowych wdrożono Zarządzeniem Nr 123/II/2019 Burmistrza Gołdapi z dnia 19 lutego 2019 r. w sprawie wprowadzenia "Polityki Ochrony Danych Osobowych" w Urzędzie Miejskim w Gołdapi (dalej: „Polityka").

Stwierdzono, iż funkcję Inspektora ochrony danych powierzono pracownikowi p. Sebastianowi Liwak[1] (dalej: „Inspektor" lub „IOD"). W wyniku analizy dokumentacji stwierdzono, iż Inspektor legitymuje się doświadczeniem w obszarze ochrony danych osobowych, dającym gwarancję poprawności realizacji zadań wynikających z pełnionej funkcji. W wyniku analizy zapisów regulaminu organizacyjnego Urzędu stwierdzono, iż treści regulacji brak jest zdefiniowanych zadań Inspektora oraz brak jest określonych zasad współpracy komórek organizacyjnych Urzędu z IOD[2].

W ocenie audytora należy rozważyć dokonanie aktualizacji zapisów regulaminu organizacyjnego Urzędu, poprzez wprowadzenie do treści regulacji funkcji Inspektora oraz zasad współpracy komórek organizacyjnych z IOD. Rekomendacja ma charakter fakultatywny.

Na poziomie Urzędu przeprowadzono przez Inspektora w dniach 16-18 października 2018 r. szkolenie w zakresie nowych przepisów ochrony danych osobowych. Stwierdzono, iż Administrator dokumentuje proces upoważniania do przetwarzania danych osobowych

[1] Umowa na świadczenie usług związanych z realizacją zadań przypisanych inspektorowi Ochrony danych w Urzędzie Miejskim w Gołdapi z dnia 31.12.2018 r. Zarządzenie Nr 1379/VII/2018 Burmistrza Gołdapi z dnia 26 lipca 2018 r. w sprawie wyznaczenie Inspektora Ochrony Danych w Urzędzie Miejskim w Gołdapi.

[2] Zarządzenie Nr 883/II/2014 Burmistrza Gołdapi z dnia 27 lutego 2014 r. w sprawie nadania Regulaminu Organizacyjnego Urzędowi Miejskiemu w Gołdapi ze zm.

w sposób, który umożliwia ustalenie wszystkich osób zaangażowanych w procesy przetwarzania danych na poziomie Urzędu. Wszystkie podmioty przetwarzające dane osobowe (w tym inne podmioty przetwarzające, które wykonują usługi na ich rzecz) zostały upoważnione przez Administratora, a przetwarzanie danych zostało powierzone w formie pisemnej. Na poziomie Urzędu dokonano inwentaryzacji umów powierzenia danych osobowych. Wypracowane w jednostce wzory umów albo klauzul umownych związanych ze świadczeniem usług przetwarzania danych osobowych są prawidłowe.

Dla wszystkich zbiorów danych/procesów przetwarzania danych zidentyfikowano podstawę prawną oraz warunki ich przetwarzania. Czynności zrealizowane przez Administratora zostały udokumentowane w rejestrze czynności przetwarzania danych osobowych. Urząd dokonał identyfikacji określonych w prawie celów przetwarzania danych osobowych.

Stwierdzono, iż na poziomie Urzędu nie dokonano identyfikacji danych osobowych, dla których podstawą przetwarzania jest zgoda. Ponadto w ocenie audytora w Urzędzie nie funkcjonuje system rejestrowania i zarządzania bieżącą zgodą na przetwarzanie danych osobowych. W treści Polityki nie określono zasad przetwarzania danych osobowych dla których podstawą ich przetwarzania jest zgoda osoby fizycznej.

W ocenie audytora, w terminie do dnia 31 grudnia 2019 r., należy dokonać aktualizacji zapisów Polityki, poprzez wprowadzenie zapisów oraz mechanizmów umożliwiających rejestrowanie i bieżące zarządzanie zgodami na przetwarzanie danych osobowych. Realizacja zalecenia powinna obejmować określenie tzw. „stanu zerowego" w zakresie rejestru zgód na przetwarzanie danych osobowych.

Na poziomie Urzędu opracowano procedurę udzielania informacji osobom, których dotyczą dane osobowe. Ponadto opracowano treść klauzuli informacyjnej dla osób, od których dane osobowe będą pozyskiwane. Treść opracowanych klauzul informacyjnych spełnia wymogi Rozporządzenia RODO. Urząd określił procedury postepowania w obszarze realizacji praw osoby, której dane dotyczą, a w szczególności w obszarze prawa dostępu do danych osobowych, sprostowania i usuwania danych osobowych, ograniczenia dostępu do danych osobowych oraz przenoszenia danych osobowych.

Stwierdzono, iż w Urzędzie funkcjonuje rejestr osób, którym nadano uprawnienia do przetwarzania danych osobowych. Rejestr obejmuje dane pracowników Urzędu oraz

pracowników okresowych (stażyści i praktykanci). W rejestrze odnotowywane są zdarzenia nadające uprawnienia do przetwarzania danych pracownikom Urzędu, jak również zdarzenia dotyczące wygaśnięcia/cofnięcia uprawnień do przetwarzania danych. Proces nadawania i cofania uprawnień jest należycie udokumentowany. Z treści upoważnienia wynika zakres dostępu do kategorii/zbiorów danych, jak również czy dane przetwarzane są w formie manualnej papierowej czy elektronicznej (w uzasadnionych przypadkach jest wskazany system lub oprogramowanie).

Urząd prowadzi ewidencję podmiotów przetwarzających dane osobowe w imieniu Administratora. Powierzenie realizacji zadań nastąpiło w formie pisemnej. Stwierdzono, iż jednostka opracowała wzór umowy powierzenia danych. Wzór dokumentu zawiera elementy wskazane w art. 28 Rozporządzenia RODO. Urząd dla wszystkich zbiorów danych/procesów przetwarzania danych zidentyfikował podstawę prawną (warunki przetwarzania). Informacja ta została zawarta w rejestrze czynności przetwarzania. W rejestrze określono:

- czynność przetwarzania,
- cele przetwarzania,
- planowane terminy usunięcia poszczególnych kategorii danych,
- opis środków technicznych i organizacyjnych,
- kategorie osób których dane dotyczą,
- kategorie osób którym dane zostaną przekazane,
- przekazanie danych do państwa trzeciego.

Administrator wyznaczył osoby właściwe w zakresie zgłaszania Prezesowi UODO naruszeń ochrony danych osobowych, które skutkują ryzykiem naruszenia praw lub wolności osób fizycznych. Urząd opracował właściwą procedurę zgłaszania i postępowania z naruszeniami ochrony danych osobowych. Na poziomie Urzędu prowadzony jest rejestr naruszeń ochrony danych osobowych, który dokumentuje w szczególności wszystkie przypadki zgłoszeń, w tym tych, które nie podlegają obowiązkowi przekazania do Prezesowi UODO.

Stwierdzono, iż na poziomie Urzędu nie dokonano identyfikacji operacji przetwarzania danych, dla których poziom ryzyka naruszenia praw lub wolności osób fizycznych oceniono, jako wysoki.

W ocenie audytora należy, w terminie do dnia 31 grudnia 2019 r., dokonać oceny skutków dla ochrony danych, zawierającej elementy określone w treści art. 35 ust. 7 Rozporządzenia RODO, tj:,

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym (gdy ma to zastosowanie) prawnie uzasadnionych interesów realizowanych przez Administratora,
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych.

Urząd opracował i ustanowił, wdrożył oraz eksploatuje, monitoruje i przegląda, utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Kompleksowa dokumentacja systemu zarządzania bezpieczeństwem informacji określona została w treści Zarządzeniem Nr 123/II/2019 Burmistrza Gołdapi z dnia 19 lutego 2019 r. w sprawie wprowadzenia "Polityki Ochrony Danych Osobowych" w Urzędzie Miejskim w Gołdapi.

Urząd posiada skrzynkę e-PUAP skonfigurowaną z systemem COIK. Wszystkie dokumenty wchodzące na skrzynkę podawczą przekazywane są do realizacji właściwych komórek organizacyjnych za pośrednictwem systemu IntraDOK. Urząd nie wykorzystuje wzorów dokumentów elektronicznych przechowywanych w Centralnym Repozytorium Wzorów Dokumentów Elektronicznych, jakie zostały już wcześniej opracowane i są używane przez inne podmioty publiczne. Jednocześnie Urząd nie przekazywał do Repozytorium wzorów dokumentów elektronicznych podmiotu publicznego.

Urząd właściwie zarządza usługami elektronicznymi w oparciu o model usługowy. Na poziomie Urzędu funkcjonuje produkt opracowany w ramach projektu „Cyfrowe usługi w zakresie udostępniania informacji publicznej Urzędu Miejskiego w Gołdapi" dofinansowanego w ramach środków Europejskiego Funduszu Rozwoju Regionalnego w ramach RPO Warmińsko-Mazurskiego 2014-2020. Zasady eksploatacji systemu, określone w dokumentacji powykonawczej z dnia 20 sierpnia 2018 r., wykorzystują model usługowy w procesie świadczenia usług elektronicznych. Pełne wdrożenie rezultatów projektu zakłada implementację usług w systemie Katalogu e- Usług, obejmujących:

- udostępnienie danych z Rejestru Dowodów Osobistych oraz dokumentacji związanej z dowodami osobistymi. Wydanie zaświadczenia z dokumentacji związanej z dowodami osobistymi,
- uzgodnienie dokumentacji technicznej i dysponowanie gruntem na cele budowlane,
- uzgodnienie lokalizacji zjazdu w pasie drogowym,
- uzgodnienie lokalizacji obiektów budowlanych lub urządzeń infrastruktury technicznej niezwiązanej z potrzebami zarządzania drogami lub potrzebami ruchu drogowego,
- wydanie zezwolenia na zajęcie pasa drogowego drogi w celu prowadzenia robót związanych z budowa lub przebudowa zjazdu,
- interwencje dot. stanów technicznych, remontów lokali i budynków stanowiących mieszkaniowy zasób gminy (miasta),
- przydział lokalu mieszkalnego,
- wydanie odpisu z rejestru stanu cywilnego,
- wniosek o wykonanie przewozów na liniach komunikacyjnych na obszarze gminy,
- wniosek o udzielnie licencji w zakresie przewozu osób i pośrednictwa,
- wniosek o nadanie awansu zawodowego nauczyciela mianowanego,
- wniosek o przyznanie pomocy materialnej o charakterze socjalnym lub zasiłku szkolnego,
- wpis do ewidencji obiektów, w których świadczone są usługi hotelarskie,
- wniosek o objęcie przedsięwzięcia patronatem honorowym Burmistrza,
- wniosek o wyrażenie zgody na używanie herbu miasta,
- wniosek o uzyskanie dotacji w ramach programu współpracy,
- zawiadomieni o zaprzestaniu wykonywania działalności gospodarczej,
- zezwolenie na sprzedaż napojów alkoholowych,
- wniosek o wydanie decyzji na zorganizowanie imprezy masowej.

Na poziomie Urzędu wykorzystywane jest system zarządzania dokumentami elektronicznymi, wpływający na uporządkowanie i usprawnienie przepływu dokumentów w Urzędzie[3]. System IntraDok firmy COIG S.A. wdrożony został w jednostce w ramach

[3] Zarządzenie Nr 1007/VII/2017 Burmistrza Gołdapi z dnia 31 lipca 2017 r. w sprawie wskazania systemu wykonania czynności kancelaryjnych, wyznaczenia koordynatora czynności kancelaryjnych oraz określenia rodzaju przesyłek wpływających, które nie są otwierane przez punkt kancelaryjny w UM w Gołdapi

projektu współfinansowanego ze środków RPO Warmińsko-Mazurskiego 2014-2020. Wdrożone narzędzie ma charakter wspomagający do tradycyjnego systemu obiegu dokumentów funkcjonującego w Urzędzie. Na dzień audytu system współpracuje z e- PUAP i docelowo będzie współpracował z modelem e-Usługi.

Urząd współdzieli informacje w sposób umożliwiający wymianę danych pomiędzy różnymi systemami informatycznymi oraz umożliwia odbiorcom swobodny dostępu do informacji, poprzez wygenerowanie danych w powszechnie znanych i dostępnych formatach plików. Urząd nie dysponuje wykazem formatów danych wykorzystywanych na poziomie systemów informatycznych Urzędu. Dokumentacja systemu IntraDok nie zawiera wykazu obsługiwanych przez system informatycznych danych. Nie stwierdzono przypadków braku możliwości przetwarzania danych przez system Intra Dok.

Stwierdzono, iż na poziomie Urzędu nie przeprowadzono okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji, obejmującej następujące elementy:

- identyfikacja ryzyka (wpływ zagrożeń na podatności),
- analiza ryzyka w tym określenie poziomu ryzyka (kombinacja prawdopodobieństwa wystąpienia i skutków/następstw),
- ocena ryzyka (porównywanie poziomu ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane),
- określenie sposobu postępowania z ryzykiem (dla ryzyka, którego wielkość jest nieakceptowalna).

Na poziomie Urzędu nie opracowano dokumentu zawierającego wyniku procesu zarządzania ryzykiem, przedstawiającego plan postępowania z ryzykiem utraty integralności, dostępności lub poufności informacji.

W ocenie audytora, w terminie do dnia 31 grudnia 2019 r., należy przeprowadzić kompleksową analizę ryzyka utraty integralności, dostępności lub poufności informacji. Proces identyfikacji, analizy i oceny ryzyka powinien być powiązany z oceną ryzyka oceny skutków dla ochrony danych, zawierającej elementy określone w treści art. 35 ust. 7 Rozporządzenia RODO.

Urząd posiada aktualny stan inwentarzowy sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Procedura ewidencjonowania urządzeń i nośników informacji zdefiniowana została w załączniku B2 do Polityki. Zgodnie

z regulacją w Urzędzie prowadzony jest rejestr urządzeń i nośników służących do przetwarzania danych osobowych. Obecnie w fazie opracowywania przez ASI jest nowe narzędzie ewidencyjne na bazie programu MS Excel.

W ocenie audytora należy rozważyć wykorzystanie ogólnodostępnego oraz darmowego oprogramowania typu „open source" umożliwiającego ewidencjonowanie urządzeń i nośników informacji. Audytor rekomenduje wykorzystanie narzędzia producent GLPI[4].

Urząd właściwie zarządza dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem zapewnia, 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, a w przypadku zmiany zadań następuje również zmiana ich uprawnień. Nie stwierdzono sytuacji, aby uprawnienia administratora wszystkich kluczowych zasobów IT posiadała jedna osoba.

Stwierdzono, iż zapisy Polityki wskazują, iż w Urzędzie uprawnione do przetwarzania danych osobowych są wyłącznie osoby upoważnione do wykonywania tych czynności. Administrator jest uprawniony do przyznawania indywidualnych upoważnień w przedmiocie przetwarzania danych osobowych. W dokumentacji w obszarze upoważnień do przetwarzania danych osobowych określono, iż nowozatrudnieni pracownicy UM, po nadaniu upoważnienia do przetwarzania danych osobowych, uczestniczą w szkoleniu prowadzonym przez IOD, mającym na celu zaznajomienie użytkownika z obowiązującymi przepisami prawa, z wewnętrzną dokumentacją obowiązującą w jednostce.

Urząd zapewnia podnoszenie świadomości zagrożeń i konsekwencji zaistnienia incydentów związanych z naruszeniem bezpieczeństwa informacji pracowników. Na poziomie Urzędu Miejskiego w Gołdapi szkoleniem z zakresu ochrony danych osobowych objęto pracowników jednostki w dniach 16-18.10.2018 r. W dokumentacji w obszarze upoważnień do przetwarzania danych osobowych określono, iż nowozatrudnieni pracownicy Urzędu, po nadaniu upoważnienia do przetwarzania danych osobowych, uczestniczą w szkoleniu prowadzonym przez IOD, mającym na celu zaznajomienie użytkownika z obowiązującymi przepisami prawa, z wewnętrzną dokumentacją obowiązującą w jednostce.

[4] https://glpi-project.org/

Urząd wprowadził regulacje wewnętrzne zawierające zasady bezpiecznej pracy użytkowników, przy wykorzystaniu urządzeń przenośnych i pracy na odległość. Zasady korzystania z komputerów przenośnych określone zostały w procedurze korzystania z komputera służbowego (załącznik B.4 Polityki). Określono zasady zabezpieczenia komputera przenośnego w czasie transportu. W procedurze wskazano zakaz logowania się do otwartych sieci (hotspoty, otwarte Wi-Fi).

Urząd zapewnił objęcie systemów informatycznych o znaczeniu krytycznym stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych). Umowy serwisowe posiadają klauzule prawne zabezpieczające bezpieczeństwo informacji, w przypadku wejścia w ich posiadanie przez podmioty zewnętrzne.

Stwierdzono, iż w regulacjach wewnętrznych Urzędu nie określono zasad zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji oraz ewentualnych zasad współpracy z cert.gov.pl, zgodnie z § 20 ust. 2 pkt 13 rozporządzenia KRI.

W ocenie audytora, w terminie do dnia 31 grudnia 2019 r., należy dokonać opracowania i wdrożenia regulacji definiujących zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji oraz ewentualnych zasad współpracy z cert.gov.pl.

Urząd zapewnia wykonywanie kopii zapasowych umożliwiających odzyskanie danych i przywrócenie do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system. Urząd wykonuje regularnie kopie zapasowe całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych. Ponadto wykonywane są regularne testy jakości kopii zapasowych, poprzez odtworzenie systemu informatycznego z kopii zwykle na niezależnym od środowiska produkcyjnego sprzętowym środowisku testowym oraz testowaniu pracy użytkowej odtworzonego systemu.

Urząd właściwie zabezpiecza informacje w sposób uniemożliwiający nieuprawnionemu ich ujawnieniu, modyfikacji, usunięciu lub zniszczeniu. Ponadto Urząd zapewnia aby w dziennikach systemów zostały odnotowane obligatoryjnie działania użytkowników lub

obiektów systemowych. Urząd zapewnia ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. W poddanych weryfikacji regulacjach wewnętrznych stwierdzono, iż ustalono w nich zasady zapewniające:

- minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, oraz urządzeń mobilnych,
- ochronę przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, poprzez ustalenie zabezpieczeń informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje usunięcie lub zniszczenie,
- monitorowanie dostępu do informacji,
- możliwość wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, poprzez kontrolę logów systemów, kontrolę wejść i wyjść do pomieszczeń serwerowni, analizę rejestru zgłoszeń serwisowych, analizę rejestru incydentów naruszenia bezpieczeństwa informacji,
- środki uniemożliwiające nieautoryzowany dostęp na poziomie systemów operacyjnych usług sieciowych i aplikacji, poprzez stosowanie systemu kontroli dostępu do pomieszczeń serwerowni, systemu autoryzacji dostępu do systemów operacyjnych, sieci i aplikacji, stosowanie systemów antywirusowych i antyspamowych, stosowanie zapór sieciowych typu firewall,
- działania związane z utylizacją sprzętu informatycznego i nośników danych a także związane z przekazywaniem sprzętu informatycznego do naprawy w sposób gwarantujący zachowanie bezpieczeństwa informacji.

Stwierdzono, iż w systemach teleinformatycznych stosowane są zabezpieczenia techniczno-organizacyjne dotyczące środowiska teleinformatycznego pracy danego systemu. ASI podejmuje działania związane z aktualizacją oprogramowania oraz redukcją ryzyka wynikającego z wykorzystywania opublikowanych podatności technicznych systemów teleinformatycznych, poprzez wdrażanie nowych wersji oprogramowania systemowego i użytkowego, poprawek i uzupełnień podnoszących ich bezpieczeństwo, aktualizację oprogramowania antywirusowego i antyspamowego, aktualizację oprogramowania zabezpieczającego ruch sieciowy, itp. Ponadto podejmowane są działania obejmujące minimalizowanie ryzyka utraty informacji w wyniku awarii oraz ochrony przed błędami, utratą i nieuprawnioną modyfikacją, a także zapewnieniem bezpieczeństwa plików

systemowych, poprzez zastosowanie bezpiecznych i redundantnych rozwiązań sprzętowych, w tym: dwustronnego bezprzerwowego zasilania, redundancji klimatyzacji, zastosowania klastra serwerów wysokiej dostępności, redundancji macierzy dyskowych i urządzeń sieciowych, równoważenie obciążenia, monitorowanie parametrów środowiskowych w serwerowni (temperatura, wilgotność, zadymienie, wyciek wody), zastosowanie systemu kopii zapasowych, systemu kontroli dostępu do zasobów informatycznych, systemu monitorowania funkcjonowania systemów teleinformatycznych i sieci.

Urząd zapewnił przetwarzanie informacji w systemach teleinformatycznych z wymogiem dostępu do danych przez uprawnione osoby i obiekty systemowe (procesy), w ustalonym zakresie. Zapewnienie rozliczalności operacji polega na gromadzeniu informacji o tym, kto, kiedy i co wykonał w systemie teleinformatycznym. Wykonywane czynności obligatoryjnie podlegają dokumentowaniu w postaci zapisów w dziennikach systemów (logi).

Stwierdzono, iż Urząd uwzględnia potrzeby osób niepełnosprawnych poprzez stosowanie w eksploatowanych systemach teleinformatycznych rozwiązań technicznych umożliwiających osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. W systemie teleinformatycznym Urzędu zapewniono spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do Rozporządzenia KRI. Zastosowane narzędzia uwzględniają rozwiązania techniczne, umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu.

Podsumowanie

Na podstawie przeprowadzonych czynności audytowych audytor wydaje ocenę pozytywną nt. funkcjonowania obszaru ochrony danych osobowych oraz spełniania wymogów KRI na poziomie Urzędu Miejskiego w Gołdapi.

Stosowane w ramach audytowanego obszaru mechanizmy kontrolne skutecznie minimalizują możliwość materializacji zagrożeń mogących mieć istotny, negatywny wpływ na realizację celów i zadań w obszarze objętym zadaniem audytowym.

W audytowanym obszarze funkcjonuje adekwatny, skuteczny i efektywny system kontroli zarządczej, z zastrzeżeniami wskazanymi w treści sprawozdania.

Zalecenia i rekomendacje

Lp.	Treść	Termin	Ryzyko
1*	Należy rozważyć dokonanie aktualizacji zapisów regulaminu organizacyjnego Urzędu, poprzez wprowadzenie do treści regulacji funkcji Inspektora oraz zasad współpracy komórek organizacyjnych z IOD.	----	Ryzyko o charakterze niskim (💣)
2	Należy dokonać aktualizacji zapisów Polityki, poprzez wprowadzenie zapisów oraz mechanizmów umożliwiających rejestrowanie i bieżące zarządzanie zgodami na przetwarzanie danych osobowych. Realizacja zalecenia powinna obejmować określenie tzw. „stanu zerowego" w zakresie rejestru zgód na przetwarzanie danych osobowych.	31 grudnia 2019	Ryzyko o charakterze średnim (💣 💣)
3	Należy dokonać oceny skutków dla ochrony danych, zawierającej elementy określone w treści art. 35 ust. 7 Rozporządzenia RODO, tj:, - systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym (gdy ma to zastosowanie) prawnie uzasadnionych interesów realizowanych przez Administratora, - ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów, - ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,	31 grudnia 2019	Ryzyko o charakterze średnim (💣 💣)

	- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych.		
4	Należy przeprowadzić kompleksową analizę ryzyka utraty integralności, dostępności lub poufności informacji. Proces identyfikacji, analizy i oceny ryzyka powinien być powiązany z oceną ryzyka oceny skutków dla ochrony danych, zawierającej elementy określone w treści art. 35 ust. 7 Rozporządzenia RODO.	31 grudnia 2019	Ryzyko o charakterze średnim (💣 💣)
5*	Należy rozważyć wykorzystanie ogólnodostępnego oraz darmowego oprogramowania typu „open source" umożliwiającego ewidencjonowanie urządzeń i nośników informacji. Audytor rekomenduje wykorzystanie narzędzia producent GLPI	----	Ryzyko o charakterze niskim (💣)
6	Należy dokonać opracowania i wdrożenia regulacji definiujących zasady zgłaszania i postępowania z incydentami naruszenia bezpieczeństwa informacji oraz ewentualnych zasad współpracy z cert.gov.pl.	31 grudnia 2019	Ryzyko o charakterze średnim (💣 💣)
Skala ryzyka: 💣 niskie, 💣 💣 średnie, 💣 💣 💣 wysokie, ⍰ krytyczne			

* - rekomendacja ma charakter fakultatywny. Decyzja o wdrożeniu rekomendacji należy do kierownika jednostki audytowanej.

Adrian Chodubski
Audytor wewnętrzny
CIAP no. 1318 MF /2008/2005

Zapoznałem się ze sprawozdaniem:
BURMISTRZ GOŁDAPI Tomasz Luto 15. 07. 2019
Burmistrz Gminy Gołdap (data i podpis)

Sekretarz Gminy Gołdap