Załącznik nr 9

do „Polityki ochrony danych osobowych”:

SZACOWANIE RYZYKA
(OGÓLNA ANALIZA I OCENA RYZYKA)
NARUSZENIA PRAW LUB WOLNOŚCI
OSÓB FIZYCZNYCH WIĄŻĄCEGO SIĘ
Z PRZETWARZANIEM DANYCH OSOBOWYCH
ORAZ OKREŚLENIE ODPOWIEDNICH ŚRODKÓW
TECHNICZNYCH I ORGANIZACYJNYCH MAJĄCYCH
ZAPEWNIĆ STOPIEŃ BEZPIECZEŃSTWA
ODPOWIADAJĄCY TEMU RYZYKU

Dokument opracowano na podstawie metodyki zalecanej przez ENISA (Europejska Agencja ds. Sieci i Bezpieczeństwa Informacji), opartej na standardzie ISO 27005: „Zagrożenia wykorzystują słabe strony aktywów, by szkodzić organizacji”, zawartej w „Podręczniku Inspektora Ochrony Danych Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasipublicznym dotyczące sposobu zapewnienia zgodności z europejskim ogólnym rozporządzeniem o ochronie danych” opublikowanym w serwisie internetowym Urzędu Ochrony Danych Osobowych.

WSTĘP

Ryzyko podlegające ocenie to nie tylko wąsko rozumiane **ryzyko bezpieczeństwa**, tj. prawdopodobieństwo i wpływ naruszenia danych, ale raczej **ryzyko dla praw i wolności osób, których dane dotyczą** (i innych jednostek), jakie może wynikać z operacji przetwarzania. Obejmuje to nie tylko ich ogólne prawa do prywatności i życia prywatnego, a także konkretne prawa osoby, której dane dotyczą, ale także w zależności od sytuacji prawo do wolności wypowiedzi, wolności przemieszczania się, wolności od dyskryminacji, wolności od władzy autorytarnej oraz prawo do życia w demokratycznym społeczeństwie bez nienależytego nadzoru ze strony swojego własnego kraju lub innych krajów i prawo do skutecznych środków prawnych.

Ocena ryzyka obejmuje cztery etapy:

1. Zdefiniowanie operacji przetwarzania i jej kontekstu.
2. Zrozumienie i ocena oddziaływania.
3. Ustalenie możliwych zagrożeń i ocena prawdopodobieństwa wystąpienia zagrożeń.
4. Ocena ryzyka (łącząca prawdopodobieństwo wystąpienia zagrożenia oraz oddziaływanie).

ETAP I: ZDEFINIOWANIE OPERACJI PRZETWARZANIA I ICH KONTEKSTU

Charakter, zakres, kontekst i cele przetwarzania danych w Urzędzie Miasta Starogard Gdański, w tym środki organizacyjne i techniczne stosowane w procesach przetwarzania określone zostały w następujących dokumentach stanowiących załączniki do „Polityki ochrony danych osobowych":

- Załącznik nr 2: *Określenie pomieszczeń tworzących w Urzędzie Miasta Starogard Gdański obszar przetwarzania danych oraz opis środków zastosowanych w celu ochrony tego obszaru*.
- Załącznik nr 3: *Opis systemu informatycznego Urzędu.*
- Załącznik nr 5: *Wykaz i opis oprogramowania wykorzystywanego do przetwarzania danych osobowych w systemach informatycznych Urzędu*.
- Załącznik nr 7: *Rejestr czynności przetwarzania danych osobowych (art. 30 ust. 1 RODO)*.
- Załącznik nr 8: *Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz podstaw prawnych legalizujących ich przetwarzanie*.
- Załącznik nr 10: *Instrukcja zarządzania systemem informatycznym*.
- Załącznik nr 11: *Opis procedur i harmonogram sporządzania kopii zapasowych*.
- Załącznik nr 13: *Procedura nadawania/zmiany/wycofywania upoważnień i uprawnień do przetwarzania danych*.
- Załącznik nr 15: *Ewidencja podmiotów (osób trzecich), którym Gmina Miasta Starogard Gdański powierzyła przetwarzanie danych osobowych oraz podmiotów (osób trzecich), które uzyskały uprawnienia dostępu do obszaru przetwarzania danych osobowych*.
- Załącznik nr 18: *Zasady przetwarzania danych osobowych w systemach monitoringu wizyjnego obowiązujące w Urzędzie Miasta Starogard Gdański.*
- Załącznik nr 20: *Zasady retencji danych osobowych*.
- Załącznik nr 25: *Dokumentacja ilustrująca częstotliwość i zakresy szkoleń osób dopuszczonych do przetwarzania danych osobowych*.

Opracowanie wyżej wskazanych dokumentów nastąpiło na podstawie dokonanego przeglądu operacji przetwarzania danych osobowych w Urzędzie Miasta Starogard Gdański.

Dla procesu dot. obsługi interesantów Urzędu opracowano odrębny dokument o nazwie „Obsługa ewidencyjna, organizacyjna i formalno-prawna spraw interesantów Urzędu".

ETAP 2: USTALENIE RÓŻNYCH POZIOMÓW ODDZIAŁYWANIA

POZIOM ODDZIAŁYWANIA	OPIS
Niski	Osoby, których dane dotyczą, mogą natrafić na kilka niewielkich niedogodności, które pokonają bez żadnych problemów (czas spędzony na ponowne wprowadzanie informacji, irytacja, rozdrażnienie, itp.).
Średni	Osoby, których dane dotyczą, mogą natrafić na znaczące niedogodności, które będą w stanie pokonać pomimo kilku trudności (dodatkowe koszty, odmowa dostępu do usług, strach, brak zrozumienia, stres, niewielkie dolegliwości fizyczne, itp.).
Wysoki	Osoby, których dane dotyczą, mogą napotkać na znaczące konsekwencje, które powinny być w stanie pokonać, aczkolwiek z poważnymi trudnościami (sprzeniewierzenie środków, umieszczenie na czarnej liście przez instytucje finansowe, szkody majątkowe, utrata pracy, wezwanie do sądu, pogorszenie stanu zdrowia, itp.).
Bardzo wysoki	Osoby, których dane dotyczą, mogą napotkać na znaczące lub nawet nieodwracalne konsekwencje, których nie są w stanie pokonać (niezdolność do pracy, długoterminowe dolegliwości psychiczne lub fizyczne, śmierć, itp.).

W aspekcie bezpieczeństwa przetwarzanych danych osobowych poddano ocenie następujące obszary:

A. Sieć i zasoby techniczne (sprzęt i oprogramowanie komputerowe).

B. Procesy/procedury związane z operacją przetwarzania danych.

C. Strony i osoby uczestniczące w operacjach przetwarzania danych.

D. Sektor działalności i skala przetwarzania.

GŁÓWNE OBSZARY OCENY BEZPIECZEŃSTWA DANYCH OSOBOWYCH

A.	**Sieć i zasoby techniczne (sprzęt i oprogramowanie komputerowe)**
1.	**Czy jakakolwiek część przetwarzania danych osobowych odbywa się przez Internet?** **TAK** Internet wykorzystywany jest przez ADO w procesach przetwarzania dotyczących: • obsługi spraw kadrowo-płacowych (korespondencja elektroniczna, transfery danych do ZUS, urzędów skarbowych, Państwowego Funduszu Osób Niepełnosprawnych), • obsługi informacji dot. interesantów poprzez dedykowane, resortowe systemy informatyczne, w tym Platformę e-PUAP, • obsługi ewidencyjnej, finansowej i organizacyjnej ADO (korespondencja elektroniczna), • obsługi ewidencyjnej i organizacyjnej korespondencji wchodzącej i wychodzącej (korespondencja elektroniczna).
2.	**Czy można zapewnić dostęp do wewnętrznego systemu przetwarzania danych osobowych przez Internet (np. dla pewnych użytkowników lub grup użytkowników)?** **TAK** Ten rodzaj dostępu przysługuje wyłącznie serwisantom oprogramowania (serwis zdalny), z zagwarantowaniem odpowiednich zabezpieczeń danych i określonych przez Administratora Systemu Informatycznego sposobów uwierzytelniania się serwisantów. Zasady w tym zakresie określone są w rozdziale 4.2.5 „Polityki ochrony danych osobowych".
3.	**Czy system przetwarzania danych osobowych jest powiązany z innym wewnętrznym (w ramach strukturyorganizacyjnej ADO) lub zewnętrznym systemem informatycznym?** **TAK** ADO wykorzystuje do przetwarzania danych osobowych systemy wyszczególnione w Załączniku nr 5 do „Polityki ochrony danych osobowych" (Wykaz i charakterystyka oprogramowania wykorzystywanego do przetwarzania danych osobowych). Do wykorzystywanych przez ADO zewnętrznych systemów należą: CEIGD – Centralna Ewidencja Informacji O Działalności Gospodarczej; ŹRÓDŁO – System teleinformatyczny służący do obsługi USC oraz obsługi dowodów osobistych; PZ – Punkt potwierdzenia profili zaufanych; Shrimp – system harmonogramowania, rejestracji i monitorowania pomocy.
4.	**Czy osoby nieupoważnione do przetwarzania danych osobowych mogą łatwo uzyskać dostęp do środowiska przetwarzania danych?** **NIE** Wdrożone zabezpieczenia i monitorowanie funkcjonowania systemu przez ASI uniemożliwiają taką ewentualność. Zabezpieczenia fizyczne obszaru przetwarzania, odpowiednia aranżacja stanowisk pracy oraz zabezpieczenia sprzętu służącego do przetwarzania danych eliminują potencjalne zagrożenia.
5.	**Czy system przetwarzania danych osobowych został zaprojektowany, wdrożony lub jest utrzymywany bez przestrzegania odpowiednich dobrych praktyk?** **NIE** System jest zaprojektowany, wdrożony i utrzymywany zgodnie ze standardami bezpieczeństwa informatycznego oraz z uwzględnieniem dobrych praktyk (zabezpieczenia fizyczne i logiczne, kontrola działań użytkowników, nadawanie i blokowanie uprawnień, systematyczne wykonywanie kopii zapasowych, nadzór nad podmiotami zewnętrznymi wykonującymi usługi serwisowe sprzętu i oprogramowania, szkolenia użytkowników).

B.	**Procesy i procedury**
6.	**Czy role i obowiązki dotyczące przetwarzania danych osobowych są niejednoznaczne lub niejasno zdefiniowane?** **NIE** Role i obowiązki uczestników procesów przetwarzania są jasno zdefiniowane, bazują na adekwatnym przydzielaniu uprawnień użytkowników systemu do zakresu kompetencji służbowych. Obowiązujące w Urzędzie zasady w tym zakresie wskazano w rozdziałach 2.1.1, 3.1-3.5, 4.1.2, 4.1.8, 4.1.9, 4.1.10, 4.2, 4.3, 4.6-4.8, 7, 8.3, 9 „Polityki". Procedura nadawania, modyfikowania i wycofywania uprawnień jest akceptowana przez Prezydenta Miasta Starogard Gdański i nadzorowana przez ASI. Użytkownicy dysponują stałym dostępem do dokumentów instrukcyjnych dot. obowiązujących w Urzędzie zasad przetwarzania danych, obowiązków użytkowników, zgłaszania incydentów naruszających bezpieczeństwo informacji (załączniki nr 17 i 23 do „Polityki ochrony danych osobowych").
7.	**Czy możliwe do zaakceptowania użytkowanie sieci, systemu i zasobów fizycznych w ramach struktury organizacyjnej ADO jest dwuznaczne lub niejasno zdefiniowane?** **NIE** Użytkowanie sieci, systemu i zasobów jest jasno zdefiniowane, bazuje na adekwatnym przydzielaniu uprawnień użytkowników do zakresu kompetencji służbowych. Procedura nadawania, modyfikowania i wycofywania uprawnień jest akceptowana przez Prezydenta Miasta Starogard Gdański i nadzorowana przez ASI. Użytkownicy dysponują stałym dostępem do dokumentów instrukcyjnych dot. obowiązujących w Urzędzie zasad przetwarzania danych, obowiązków użytkowników, zgłaszania incydentów naruszających bezpieczeństwo informacji (załączniki nr 17 i 23 do „Polityki ochrony danych osobowych").
8.	**Czy pracownikom wolno wnosić i użytkować swoje własne urządzenia podłączone do systemu przetwarzani danych osobowych?** **NIE** Obowiązuje zakaz w tym zakresie sformułowany w rozdziale 3.1.2 „Polityki ochrony danych osobowych" oraz w obowiązującym w Urzędzie i dostępnym dla każdego użytkownika systemu dokumencie instrukcyjnym o nazwie „Zasady przetwarzania danych osobowych w Urzędzie Miasta Starogard Gdański" (załącznik nr 17 do „Polityki ochrony danych osobowych".
9.	**Czy pracownikom wolno przekazywać, przechowywać lub w inny sposób przetwarzać dane osobowe poza obszarem przetwarzania danych określonym przez ADO?** **TAK** Wyłącznie osobom upoważnionym, z zagwarantowaniem odpowiednich zabezpieczeń danych i określonych przez Administratora Systemu Informatycznego sposobów uwierzytelniania się użytkownika (w przypadku przetwarzania danych przy wykorzystaniu komputerów stacjonarnych / sprzętu mobilnego – patrz: Załącznik nr 19 do „Polityki" o nazwie „Szczegółowe zasady przetwarzania danych osobowych poza obszarem administracyjnym Zakładu").
10.	**Czy czynności przetwarzania danych mogą być wykonywane bez utworzenia plików dziennika?** **NIE** ASI prowadzi dzienniki pracy serwerów.
C.	**Strony i osoby uczestniczące w operacjach przetwarzania**
11.	**Czy przetwarzanie danych wykonywane jest przez nieokreśloną liczbę pracowników?** **NIE** Przetwarzaniem danych zajmuje się określona i nadzorowana liczba osób upoważnionych zgodnie z procedurą określoną w rozdziałach 3.3, 4.2 i 4.3 „Polityki ochrony danych osobowych" oraz w Załączniku nr 13 do „Polityki" o nazwie „Procedura nadawania / zmiany / wycofywania upoważnień i uprawnień do przetwarzania danych osobowych".
12.	**Czy jakakolwiek część operacji przetwarzania danych wykonywana jest przez wykonawcę / stronę trzecią (podmiot przetwarzający dane)?** **TAK** Podmioty zewnętrzne realizują działania na danych osobowych Urzędu w następującym zakresie.: • serwisowanie i aktualizowanie oprogramowania, • serwisowanie urządzeń wchodzących w skład systemu informatycznego. Wykaz tych podmiotów i zawartych z nimi umów powierzenia zawiera Załącznik nr 15 do „Polityki".
13.	**Czy obowiązki osób / stron uczestniczących w przetwarzaniu danych osobowych są niejednoznaczne lub niejasno ustalone?** **NIE** Role i obowiązki uczestników procesów przetwarzania są jasno zdefiniowane, bazują na adekwatnym przydzielaniu uprawnień użytkowników systemu do zakresu kompetencji służbowych. Procedura nadawania, modyfikowania i wycofywania uprawnień jest akceptowana przez Prezydenta Miasta Starogard Gdański i nadzorowana przez ASI. Użytkownicy dysponują stałym dostępem do dokumentów instrukcyjnych dot. obowiązujących w Urzędzie zasad przetwarzania danych, obowiązków użytkowników, zgłaszania incydentów naruszających bezpieczeństwo informacji (załączniki nr 17 i 23 do „Polityki ochrony danych osobowych"). Zasady doboru podmiotów, którym ADO powierzył przetwarzanie danych osobowych i nadzorowania sposobów wykonywania przez nie powierzonych zadań określają rozdziały 3.4 i 3.5 „Polityki".
14.	**Czy pracownicy uczestniczący w przetwarzaniu danych osobowych nie znają określonych przez ADO zasadybezpieczeństwa informacji?** **NIE** Osoby dopuszczone do przetwarzania danych osobowych są zapoznane z określonymi przez ADO zasadami bezpieczeństwa informacji poprzez dysponowanie stałym dostępem do dokumentów instrukcyjnych dot. obowiązujących w Zakładzie zasad przetwarzania danych, obowiązków użytkowników, zgłaszania incydentów naruszających bezpieczeństwo informacji (załączniki nr 14 i 15 do „Polityki") oraz udział w szkoleniach prowadzonych przez specjalistów zewnętrznych, jak też ASI.
15.	**Czy osoby / strony uczestniczące w operacji przetwarzania danych zaniedbują zasady bezpiecznego przechowywania i / lub niszczenia danych osobowych?** **NIE** Nie stwierdzono takich przypadków. ASI monitoruje bezpieczne funkcjonowanie sieci i systemu oraz działania użytkowników systemu. Osoby dopuszczone przez ADO do przetwarzania danych dysponują stałym dostępem do dokumentów instrukcyjnych dot. obowiązujących w Urzędzie zasad przetwarzania danych, obowiązków użytkowników, zgłaszania incydentów naruszających bezpieczeństwo informacji (załączniki nr 17 i 23 do „Polityki").

D.	Sektor działalności i skala przetwarzania
16.	**Czy można uznać sektor działalności ADO za podatny na cyberataki?** **TAK** Realia przetwarzania danych przez ADO powodują podatność na cyberataki.
17.	**Czy ADO ucierpiał z powodu cyberataku lub innego naruszenia bezpieczeństwa w ciągu ostatnich dwóch lat?** **NIE**
18.	**Czy w ostatnim roku ADO otrzymał zgłoszenia i / lub skargi dotyczące bezpieczeństwa systemu informatycznego wykorzystywanego do przetwarzania danych osobowych?** **NIE** Nie wpłynęły do ADO zgłoszenia lub skargi dot. bezpieczeństwa systemu informatycznego.
19.	**Czy operacja przetwarzania dotyczy dużej ilości podmiotów danych i / lub danych osobowych?** **NIE** W ramach przyjętej metodyki określa się następujące szacowanie ilości danych: • **znikoma** – pojedyncze rekordy, • **mało** – informacje maksymalnie o kilkuset tysiącach osób, • **dużo** – informacje liczone w milionach rekordów, • **bardzo dużo** – dane o kilkunastu milionach osób i więcej.
20.	**Czy istnieją jakiekolwiek dobre praktyki z zakresu bezpieczeństwa dotyczące konkretnie sektora działalności ADO, które nie są właściwie stosowane?** **NIE** ADO wykorzystuje dostępne rozwiązania organizacyjno-techniczne, jak też dobre praktyki określone w normach bezpieczeństwa informatycznego.

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA (1)

Obszar oceny:	Liczba odpowiedzi „tak”	Poziom	Wynik
Sieć i zasoby techniczne	**0-1**	**Niski**	**1**
	2-3	**Średni**	**2**
	4-5	**Wysoki**	**3**
Procesy i procedury	**0-1**	**Niski**	**1**
	2-3	**Średni**	**2**
	4-5	**Wysoki**	**3**
Osoby i strony zaanga-żowane w operację	**0-1**	**Niski**	**1**
	2-3	**Średni**	**2**
	4-5	**Wysoki**	**3**
Sektor i skala przetwa-rzania	**0-1**	**Niski**	**1**
	2-3	**Średni**	**2**
	4-5	**Wysoki**	**3**

Na podstawie powyżej otrzymanych wyników podsumowano prawdopodobieństwo wystąpienia zagrożenia:

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA (2)

Ogólna SUMA wyników:	POZIOM PRAWDOPODOBIEŃSTWA wystąpienia zagrożenia:
4-5	**Niski**
6-8	**Średni**
9-12	**Wysoki**

Wynik prawdopodobieństwa wystąpienia zagrożenia („średni”) połączony z określonymi na pierwszym schemacie wynikami „poziomu oddziaływania”, wskazuje ogólne ryzyko:

OGÓLNA OCENA RYZYKA

	POZIOM ODDZIAŁYWANIA			
PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA		Niskie	Średnie	Wysokie / Bardzo Wysokie
	Niskie			
	Średnie			
	Wysokie			

Legenda:

Niskie ryzyko

Średnie ryzyko

Wysokie ryzyko

OCENA RYZYKA

Na podstawie przeprowadzonego szacowania ryzyka zidentyfikowano najgroźniejsze ryzyka w związku z przetwarzaniem w Urzędzie Miasta Starogard Gdański danych osobowych w ramach następujących procesów:

- rekrutacja pracowników;
- obsługa spraw kadrowo-płacowych;
- obsługa ewidencyjna, finansowa i organizacyjna klientów i kontrahentów;
- przechowywania informacji archiwalnych;
- zapisy wizyjne;
- obsługa ewidencyjna i organizacyjna bazy kontaktów.

Dokonane szacowanie pozwala wnioskować, że wielkość ryzyka dla przetwarzania danych we wskazanych zasobach Urzędu jest **ŚREDNIA**. Występujące ryzyka są akceptowalne, nie wymagają obecnie dalszego postępowania.

WNIOSKI I PRZEDSIĘWZIĘCIA

1. Analiza ryzyka pozwoliła na określenie potrzeb w zakresie zabezpieczenia przetwarzanych danych, w tym zasobów systemu informatycznego, co jest istotnym czynnikiem wpływającym na efektywność zastosowanych środków ochrony.
2. Istotne znaczenie dla ryzyka naruszenia praw lub wolności osób fizycznych wiążącego się z przetwarzaniem danych osobowych ma okres przechowywania danych w zasobach papierowych i informatycznych. O ile bezproblemowe jest usuwanie (archiwizowanie lub niszczenie) danych utrwalonych na nośnikach papierowych, o tyle skuteczne usunięcie tych danych z nośników informatycznych wymaga przygotowania odpowiednich narzędzi informatycznych. W celu respektowania zasady ograniczenia czasowego przetwarzania danych ADO wykorzystywał będzie narzędzia informatyczne przygotowywane przez autorów oprogramowania wykorzystywanego do przetwarzania danych osobowych.
3. Kierownictwo służbowe Urzędu zwracać winno szczególną uwagę na przestrzeganie przez personel zasad stosowania środków zabezpieczających przetwarzane dane, w tym dbałość o przechowywanie po godzinach pracy nośników papierowych i informatycznych zawierających dane osobowe w szafach zamykane na klucze.
4. Równolegle z dbałością o zorganizowanie i utrzymanie systemu ochrony danych zapewniającego bezpieczeństwo przetwarzanym danym należy dostrzegać konieczność przeprowadzania okresowych szkoleń mających na celu podniesienie ogólnej świadomości w zakresie zapewniania danym bezpieczeństwa, przestrzegania wypracowanych procedur oraz ukształtowania właściwych nawyków użytkowników systemu.
5. Uwzględniając wyniki szacowania ryzyka należy wskazać, że utrzymanie pożądanego poziomu bezpieczeństwa danych przetwarzanych w strukturach ADO można uzyskać poprzez:
   - wprowadzenie przeglądów ryzyk oraz stanu bezpieczeństwa w okresach nieprzekraczających **12 miesięcy**,
   - zapewnienie prawidłowej i bezpiecznej eksploatacji systemu poprzez systematyczne konserwacje sprzętu oraz aktualizacje oprogramowania,
   - systematyczne tworzenie kopii zapasowych i ich bezpieczne przechowywanie,
   - wdrożenie odpowiednich zabezpieczeń systemu informatycznego,
   - konsekwentne wdrażanie postanowień procedur określających nadawanie uprawnień do pracy w systemach oraz zasad pracy z danymi zapewniających im bezpieczeństwo,
   - utrzymywanie aktualności ewidencji osób dopuszczonych do przetwarzania danych,
   - wdrożenie i doskonalenie procedur postępowania w przypadku naruszenia ochrony danych osobowych,

- zobligowanie IOD i ASI do sprawowania nadzoru nad przestrzeganiem w Urzędzie przepisów RODO oraz procedur określonych w „Polityce ochrony danych osobowych”,
- przeprowadzanie okresowych szkoleń osób dopuszczonych do przetwarzania danych,
- reagowanie na incydenty naruszenia bezpieczeństwa informacji, w tym ich dokumentowanie, wyjaśnianie oraz w uzasadnionych prawnie przypadkach zgłaszanie Prezesowi Urzędu Ochrony Danych Osobowych.

6. Wyżej sformułowane propozycje nie wymagają istotnych nakładów finansowych, poza wygospodarowaniem środków na okresowe audyty i szkolenia zewnętrzne.
7. W celu zminimalizowania zagrożeń ciężar nadzoru nad prawidłowym i bezpiecznym funkcjonowaniem systemu ochrony danych osobowych spoczywał będzie na:
   - Inspektorze Ochrony Danych,
   - Administratorze Systemu Informatycznego,
   - wskazanych przez Prezydenta Miasta Starogard Gdański osobach funkcyjnych.

Osoby te zapewniały będą wykonywanie zadań związanych z minimalizowaniem ryzyka poprzez prowadzenie systematycznego nadzoru zabezpieczeń, procedur, sprzętu i oprogramowania.

Z powyższymi wnioskami i propozycjami zapoznałem się.
Wszystkie propozycje akceptuję i nakazuję ich realizację.

.....
(Prezydent Miasta Starogard Gdański)

RYZYKA SZCZĄTKOWE

Dane osobowe przetwarzane są w Urzędzie za pomocą odpowiednio dobranych środków technicznych i organizacyjnych w sposób zapewniający im właściwy poziom bezpieczeństwa przed przypadkową utratą, zniszczeniem, uszkodzeniem, nieuprawnioną modyfikacją, w tym ochronę przed przetwarzaniem niezgodnym z prawem. Konieczne jest, bez względu na okoliczność ocenienia ryzyka na poziomie niskim, poddawanie go szczegółowej ocenie podczas kolejnych, cyklicznych analiz. W wyniku przeprowadzonej analizy ryzyka stwierdzono, że zabezpieczenia istniejące lub zastosowane (zmodyfikowane) po dokonanym oszacowaniu skutecznie obniżają poziom ryzyka. Do zabezpieczeń tych należą:

środki ochrony fizycznej (czynnej):

- wykorzystywanie środków zabezpieczających pomieszczenia wykorzystywane do przetwarzania danych osobowych (realizacja działań profilaktycznych, ustaleniowych i ochronnych w uzasadnionych sytuacjach),
- wykorzystywanie środków zabezpieczających gwarantowanych przez podmioty, którym Administrator Danych powierzył przetwarzanie danych osobowych (realizacja działań profilaktycznych, ustaleniowych i ochronnych w uzasadnionych sytuacjach);

środki ochrony budowlano-mechaniczne - ściany i stropy budynków, drzwi, okna, szyby, zamki, kłódki, sejfy, zamykane szafy do przechowywania nośników;

środki ochrony elektronicznej – system sygnalizacji włamania oraz system telewizji dozorowej;

środki ochrony elektromagnetycznej - urządzenia wykonane w odpowiedniej kategorii (standardzie);

środki ochrony antywirusowej - licencjonowane oprogramowanie, procedury postępowania w przypadku wystąpienia incydentu, w tym procedury przywracania prawidłowego funkcjonowania systemu i odtwarzania danych z kopii zapasowych;

środki ochrony informatycznej - licencjonowane oprogramowanie systemowe, użytkowe, procedury tworzenia kopii zapasowych i ich sprawdzania, szkolenia użytkowników systemu, nadzór nad ich działaniami w systemie;

środki ochrony przeciwpożarowej – sprzęt gaśniczy i jego właściwe rozmieszczenie;

procedury organizacyjne - nadzór nad przestrzeganiem zasad „czystego biurka" i „czystego ekranu", zamykanie drzwi i okien w pomieszczeniach po zakończonej pracy, zarządzanie kluczami do pomieszczeń, nadzór nad pracą serwisantów urządzeń oraz personelem sprzątającym pomieszczenia biurowe, system tworzenia i przechowywania kopii zapasowych, zasady przechowywania dokumentacji technicznej dot. zasilania, okablowania, sprzętu, oprogramowania, planów awaryjnych oraz planów ciągłości działania,

odpowiednia polityka kadrowa - osoby dopuszczone do przetwarzania danych są odpowiednio przeszkolone w tym zakresie, jak też objęte są procedurami nadawania uprawnień do pracy w systemie informatycznym.

Po zwróceniu uwagi na każdy z aspektów związanych ze wskazanymi powyżej środkami zabezpieczającymi oraz po dokonaniu wnikliwej analizy zagrożeń i podatności wszystkich czynników istnieje nadal pewne ryzyko dla bezpieczeństwa zasobów. Zdefiniowano ryzyka występujące w systemie z zaznaczeniem, że są one znane i akceptowalne.

- Możliwe jest zaistnienie sytuacji wynikających ze zbiegu kilku zagrożeń w jednym czasie, np. nastąpi awaria zasilania, a użytkownik nie przestrzega zasady okresowego zapisywania danych. Eliminacja ryzyk tego rodzaju możliwa jest w zasadzie tylko poprzez intensyfikację właściwie przeprowadzanych szkoleń użytkowników.
- Innym zagrożeniem są możliwe przypadki ujawnienia informacji chronionych przez obecnych lub byłych pracowników zorientowanych w systemach i procedurach zabezpieczeń, nie można też wykluczyć że informacje chronione mogą usiłować pozyskać osoby występujące w rolach interesantów / kontrahentów.
- Potencjalnym obszarem niebezpieczeństw są awarie lub pożar urządzeń technicznych wskutek działania sił przyrody, niedbalstwa, przypadku lub celowego działania ludzkiego o znamionach przestępstwa. Nie można wykluczyć wystąpienia kilku awarii sekwencyjnych - w konsekwencji wyłączających wykorzystywany system bezpieczeństwa informacji przez okres dłuższy niż przewidziany (przyjęty), jako dopuszczalny.

Należy mieć świadomość, że określonych ryzyk nigdy całkowicie nie zlikwidujemy. Należą one do grupy ryzyk szczątkowych, które zgodnie z przyjętymi kryteriami mogą zostać zaakceptowane przez Dyrektora SP ZOZ w Czersku.

AKCEPTACJA RYZYK

przez Prezydenta Miasta Starogard Gdański

Zgodnie z ustaleniami zawartymi w Normie PN-EN ISO/IEC 27001:2017-06 - wersja polska - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania, po zapoznaniu się z wynikami procesu szacowania ryzyka oraz ryzykami szczątkowymi po wprowadzeniu zabezpieczeń

AKCEPTUJĘ ryzyka szczątkowe wraz z ich ewentualnymi konsekwencjami:

.....

(Prezydent Miasta Starogard Gdański)