

ZARZĄDZENIE NR 40/2018

STAROSTY ŁOWICKIEGO

z dnia 13 maja 2018 r.

**w sprawie wprowadzenia Analizy zagrożeń i ryzyka przetwarzania danych osobowych
w Starostwie Powiatowym w Łowiczu**

Na podstawie art. 32 ust 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 679/2016 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 (Dz. Urz. UE L 119/1) oraz art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j. Dz. U. z 2018 r., poz. 995), zarządzam, co następuje:

§1. Wprowadzam *Analizę zagrożeń i ryzyka przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu*, stanowiącą załącznik do niniejszego zarządzenia.

§2. Nadzór nad wykonaniem zarządzenia powierzam Inspektorowi Ochrony Danych w Starostwie Powiatowym w Łowiczu.

§3. Traci moc zarządzenie Nr 37/2016 Starosty Łowickiego z dnia 19 maja 2016 r. w sprawie wprowadzenia Analizy zagrożeń i ryzyka przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu.

§4. Zarządzenie wchodzi w życie z dniem 25 maja 2018 r.

STAROSTA ŁOWICKI

Krzysztof Figat

Administrator
Bezpieczeństwa Informacji

Martyna Bogucka

RADCA PRAWNY

Anna Motuś
Łd-M-1619

Załącznik
do Zarządzenia Nr 40/2018
Starosty Łowickiego
z dnia 23 maja 2018 r.
w sprawie wprowadzenia
Analizy zagrożeń i ryzyka przetwarzania danych
osobowych w Starostwie Powiatowym w Łowiczu

ANALIZA ZAGROŻEŃ I RYZYKA PRZETWARZANIA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W ŁOWICZU

PODSTAWY PRAWNE

§1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 679/2016 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 (Dz. Urz. UE L 119/1).

WYMOGI OGÓLNE BEZPIECZEŃSTWA

§2. Celem Starostwa Powiatowego w Łowiczu jest bezpieczne i prawidłowe przetwarzanie danych osobowych, w tym w systemach informatycznych.

§3. Wszystkie działania podejmowane w sferze administracyjnej i gospodarczej, niewypełnienie obowiązków prawnych w działalności bieżącej jest obciążone ryzykiem operacyjnym.

§4. Ryzyko strat w wyniku błędnego czy niewłaściwie działającego procesu zarządzania Starostwem, wpływ czynnika ludzkiego, sprawność systemów teleinformatycznych oraz wpływ wydarzeń pochodzących z zewnątrz jednostki wpływa bezpośrednio wykonywanie ustawowych zadań przez Starostwo Powiatowe w Łowiczu.

§5. Przetwarzanie danych osobowych wpisane jest w ryzyko operacyjne, w ramach którego jest przeprowadzana analiza ryzyka. Proces ten obejmuje identyfikację i ocenę zagrożeń związanych z przetwarzaniem danych osobowych, z uwzględnieniem kategorii danych.

§6. Naruszenie bezpieczeństwa może nastąpić poprzez spełnienie potencjalnego dotąd ryzyka utraty aktywów w postaci kluczowych zasobów lub utraty nad nimi kontroli. Wszystkie podejmowane działania wiążą się z ograniczaniem ryzyka, wyeliminowaniem jego nieakceptowanego poziomu utraty zasobu. Zabezpieczenie jako reguła racjonalności jest prewencją pozwalającą na zachowanie ciągłości pracy Starostwa. Odstępstwo od tej reguły może wynikać tylko z przepisów prawa.

§7. Racjonalność zastosowanych zabezpieczeń przejawia się tym, że Administrator danych osobowych, zwany dalej Administratorem, ma świadomość zawodności materiałów, urządzeń, technologii i na końcu ludzkiej niedoskonałości.

§8. Szacowanie ryzyka jest procesem ciągłym, wykonywanym raz w roku przez Inspektora i ASI, w miesiącu wrześniu lub niezwłocznie w przypadku pojawienia się nowych zagrożeń. Wyniki przedstawiane są Administratorowi do decyzji, z uwzględnieniem zapisów § 27.

§9. Nie będzie akceptowana niekompetencja pracowników, w tym nieznanostwo prawa, błąd ludzki, w tym lekceważenie prawa, ani świadome czy szkodliwe działanie pracownika. Każdy incydent z tym związany będzie indywidualnie analizowany przez Inspektora i ASI, a wniosek zostanie przedłożony do decyzji Administratora.

§10. Przetwarzanie danych osobowych w Starostwie Powiatowym w Łowiczu i związane z tym informacje występują w postaci:

- 1) plików lub informacji przechowywanych na dysku twardym komputera;
- 2) plików lub informacji przechowywanych w pamięci operacyjnej komputera;
- 3) plików lub informacji zapisywanych na nośnikach komputerowych;
- 4) gotowych dokumentów lub wersji roboczych wydrukowanych na papierze.

§11. Bezpieczeństwo przetwarzanych bądź przechowywanych informacji zawierających dane osobowe wymaga:

- 1) zapewnienia ochrony fizycznej stanowiska komputerowego przed nieuprawnionym dostępem;
- 2) ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu komputerowego, w tym zasad postępowania nimi przed nieuprawnionym dostępem;

- 3) zabezpieczenia przed nieuprawnionym dostępem do danych osobowych znajdujących się w systemie informatycznym;
- 4) zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego tylko dla upoważnionych użytkowników;
- 5) zapewnienie możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności;
- 6) zapewnienie kontroli nośników, na których przechowuje się dane osobowe.

ZAGROŻENIA DLA SYSTEMU

§12. System informatyczny, który służy do przygotowania dokumentów zawierających dane osobowe jest podatny na zagrożenia wystąpienia incydentu powodującego utratę:

- 1) **poufności** – właściwość zapewniająca, że dane osobowe nie są udostępniane nieupoważnionym podmiotom;
- 2) **rozliczalność** – działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- 3) **integralności** - dane osobowe nie zostały w sposób nieuprawniony zmienione, zniszczone w sposób nieautoryzowany.

POUFNOŚĆ

§13. Zagrożenia w zakresie poufności obejmują:

- 1) nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe;
- 2) ujawnienie haseł dostępu do stanowiska komputerowego na którym przetwarzane są dane osobowe;
- 3) nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik;
- 4) utrata nośnika zawierającego dane osobowe;
- 5) klęska żywiołowa, w wyniku której utracono poufność danych osobowych;
- 6) nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym;
- 7) podsłuch i podgląd danych osobowych;
- 8) niekontrolowane wynoszenie danych poza obszar przetwarzania;
- 9) pokonanie zabezpieczeń fizycznych bądź programowych;
- 10) naprawy i konserwacja systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych.

ROZLICZALNOŚĆ

§14. Zagrożenia w zakresie rozliczalności obejmują:

- 1) brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania;
- 2) brak możliwości identyfikacji użytkownika na stanowisku komputerowym gdzie przetwarza się dane osobowe, indywidualne identyfikatory, rejestr użytkowników ;
- 3) nieuprawnione wprowadzenie zmian w treści dokumentu zawierającego dane osobowe;
- 4) błędy oprogramowania lub sprzętu, niewłaściwa konfiguracja systemu informatycznego;
- 5) błędy w administrowaniu systemem informatycznym;
- 6) niespełnianie przez system informatyczny wymagań ustawowych;
- 7) brak rejestracji udostępniania danych osobowych.

INTEGRALNOŚĆ

§15. Zagrożenia w zakresie integralności obejmują:

- 1) nielegalny dostęp danych osobowych, w tym do stanowiska komputerowego;
- 2) błędy, pomyłki;
- 3) brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika;
- 4) wadliwe działanie systemu operacyjnego;
- 5) wirus;
- 6) brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych;
- 7) zagrożenia zewnętrzne.

§16. Źródłami zagrożeń dla stanowisk komputerowych, gdzie przetwarza się dane osobowe mogą być:

- 1) siły natury, zdarzenia nie wynikające z działalności człowieka:
 - a) uderzenia pioruna,
 - b) pożar, konsekwencja uderzenia pioruna,
 - c) starzenie się sprzętu,
 - d) starzenie się nośników pamięci,
 - e) smog, kurz,
 - f) katastrofy budowlane,
 - g) ulewny deszcz,
 - h) huragan,
 - i) ekstremalne temperatury, wilgotność,
 - j) epidemia;
- 2) ludzie, mogą to być pracownicy, osoby z zewnątrz urzędu, którzy działają w sposób celowy lub przypadkowy:
 - a) błędy i pomyłki użytkowników,
 - b) błędy i pomyłki administratorów,
 - c) błędy w utrzymaniu systemu w poufności integralności i rozliczalności,
 - d) zaniedbania użytkowników w kopiowaniu przesyłaniu udostępnianiu,
 - e) zgubienie nośnika,
 - f) zniszczenie nośnika, niewłaściwe zniszczenie,
 - g) choroba ważnych osób,
 - h) podpalenie obiektu,
 - i) niedobór kadry, brak osób uprawnionych do dostępu do pomieszczeń i danych,
 - j) zalanie wodą,
 - k) katastrofa budowlana, przypadkowe działanie człowieka,
 - l) zakłócenia elektromagnetyczne, radiotechniczne,
 - m) podłożenie bomby, wybuch,
 - n) użycie broni,
 - o) utrata prądu,
 - p) zmiany napięcia w sieci,
 - q) niedobór pracowników,
 - r) utrata kluczowych pracowników,
 - s) szpiegostwo,
 - t) wandalizm,
 - u) kradzież,
 - v) wyłudzenie,
 - w) włamanie,
 - x) podsłuch,
 - y) podszycie się pod inną osobę,
 - z) użycie złośliwego oprogramowania,
 - aa) włamanie do systemu,

§17. Każde z zagrożeń wynikających z działalności człowieka może być ograniczone poprzez:

- 1) rygorystyczne przestrzeganie zasad postępowania z danymi osobowymi;
- 2) fizyczne zabezpieczenie obiektu, w którym działa system;
- 3) wdrożenie systemu kontroli użytkowników;
- 4) szkolenia.

§18. Zagrożenia wynikające z działania sił natury można ograniczyć poprzez właściwe zabezpieczenie budynków i pomieszczeń, w których znajdują się stanowiska komputerowe, na których przetwarza się dane osobowe.

STOPIEŃ WAŻNOŚCI INFORMACJI

§19. Stopień ważności informacji zawierających dane osobowe określa poziom ochrony oraz zastosowanie właściwych środków bezpieczeństwa. W Starostwie Powiatowym w Łowiczu został określony jako poziom wysoki.

§20. W Starostwie przetwarzane są dane osobowe tzw. dane osobowe „zwykłe” oraz dane osobowe „wrażliwe”. Przeważająca część dokumentów i informacji dotyczących danych osobowych jest wykonywana przy pomocy komputerów i wielkość strat i skutków ujawnienia bądź utraty informacji jest stosunkowo duża.

§21. Poziom utraty poufności jest wysoki i ustalony na poziomie 8-9 w skali 10 stopniowej.

§22. Wymagania związane z zachowaniem rozliczalności określono jako średnie 4-6 punktów w skali 10 punktowej.

§23. Zachowanie integralności informacji zawierających dane osobowe określono na wysokie na poziomie 8-9 w skali 10 punktowej.

PODATNOŚĆ SYSTEMU NA ZAGROŻENIA

§24. Podatność systemu na zagrożenia może wynikać z:

- 1) dostępności systemu wynikającego np. z braku ochrony fizycznej budynku lub znacznej liczby personelu, mającego potencjalnie dostęp do systemu oraz wiedzę jak obsługiwać system;
- 2) dostępność informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych;
- 3) możliwość celowego wprowadzania luk w sprzęcie i oprogramowaniu lub wprowadzania wirusów komputerowych;
- 4) możliwość awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślną interwencję;
- 5) przesyłanie informacji przez niezabezpieczone łącza telekomunikacyjne.

§25. Podatność systemu na zagrożenia została ograniczona poprzez:

- 1) ochronę fizyczną stanowisk komputerowych;
- 2) kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe, wydzielenie stref ochronnych;
- 3) ograniczenie liczby personelu, mającego potencjalnie dostęp do stanowisk komputerowych oraz wiedzę jak je obsługiwać;
- 4) przeglądy okresowe nośników;
- 5) kontrolę zmian konfiguracji;
- 6) testowanie oprogramowania;
- 7) audyt;

- 8) zabezpieczanie haseł;
- 9) użycie oprogramowania antywirusowego;
- 10) backupy.

ANALIZA ZAGROŻEŃ I RYZYKA

§26. Działania w celu przygotowania reakcji na ryzyko podejmowane są według poniższego schematu:

- 1) identyfikacja ryzyka, jako proces polegający na:
 - a) określeniu zasobów/aktywów,
 - b) określeniu zagrożenia dla zasobów oraz ich podatność, które mogą być wykorzystane przez zagrożenia,
 - c) określeniu skutków jakie mogą wystąpić w stosunku do zasobów w przypadku utraty poufności, integralności i rozliczności;
- 2) oszacowanie ryzyka, jako proces polegający na:
 - a) oszacowaniu strat szkód powstałych z naruszeniem bezpieczeństwa, biorąc pod uwagę konsekwencje utraty: poufności, integralności i rozliczności,
 - b) oszacowaniu realnego prawdopodobieństwa zdarzenia takiego naruszenia,
 - c) wyznaczeniu poziomu ryzyk,
 - d) stwierdzeniu, czy ryzyko jest akceptowalne lub tolerowane, czy też nieakceptowane i wymaga podjęcia działania;
- 3) postępowanie z ryzykiem, jako plan działania polegający na wyborze metody postępowania z ryzykiem:
 - a) **zabezpieczenie** - zastosowanie odpowiednich zabezpieczeń,
 - b) **zaakceptowanie zidentyfikowanych ryzyk** - w sposób świadomy i obiektywny przy założeniu że jasno spełniają warunki wyznaczone w polityce bezpieczeństwa i/oraz kryteria akceptowania ryzyk,
 - c) **unikanie ryzyk** - poprzez przeniesienie, wycofanie, reakcja.

§27. W celu oszacowania potencjalnych strat wynikających z utraty (ujawnienia) danych osobowych przetwarzanych w Starostwie Powiatowym w Łowiczu, w tym na stanowiskach komputerowych wykonuje się analizę z określeniem przewidywanych zagrożeń dla zasobów, zgodnie z załącznikiem nr 1. Zidentyfikowane zagrożenia w obszarze przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu opisano w załączniku nr 2 do niniejszego dokumentu, stanowiący katalog otwarty i modyfikowalny.

§28. W celu oszacowania ryzyka stosujemy załącznik nr 3 do niniejszego dokumentu pt. *Macierz szacowania ryzyka*. Wyniki są przekazywane w formie sprawozdania dla Administratora, według wzoru określonego w załączniku nr 4 do niniejszej dokumentu.

§29. Określono akceptowalny poziom ryzyka na poziomie średnim.

§30. Do każdego nieakceptowanego poziomu ryzyka Administrator podejmuje decyzję określającą zastosowanie działań:

- 1) decyzja akceptująca ryzyko, gdy działania są niemożliwe do realizacji lub są zbyt kosztowne;
- 2) decyzja w sprawie transferu ryzyka, np. ubezpieczenie, przeniesienie na inny podmiot;
- 3) decyzja- podjęcie działań w celu zmniejszenia ryzyka do akceptowalnego poziomu.

WNIOSKI

§31. Wyniki z przeprowadzonej analizy są podstawą do przygotowania stosownej dokumentacji lub zmiany zapisów w obowiązujących dokumentach dotyczących bezpieczeństwa przetwarzania danych osobowych w Urzędzie, w tym reorganizacji jego struktur. Stanowią również podstawę wniosku o dostosowanie systemów informatycznych do zachowania bezpieczeństwa przetwarzania danych osobowych i bezpieczeństwa informacji.

§32. Inspektor Ochrony Danych, z przeprowadzonej wraz z ASI, analizy zagrożeń i ryzyka, przedkłada Administratorowi sprawozdanie, o którym mowa w §29 wraz z wnioskami propozycji działania w odniesieniu do nieakceptowanych, zidentyfikowanych ryzyk. Sprawozdanie jest przedkładane w terminie do dwóch tygodni od jej wykonania. W sytuacji opisanej w §9, pojawienia się nowych zagrożeń, termin ulega skróceniu do 5 dni.

§33. Przeprowadzona analiza, jej wyniki oraz sprawozdanie przedkładane Administratorowi są informacjami do użytku wewnętrznego.

STAROSTA ŁOWICKI

Krzysztof Figat

Podstawowe zasady analizy zagrożeń i ryzyka

- 1) Określamy:
 - a) Zasoby/ aktywa, które będziemy chronić,
 - b) Zagrożenia -czynniki, które mogą spowodować wystąpienie incydentu,
 - c) Prawdopodobieństwo- podatność, słabość zasobu, możliwość wykorzystania przez zagrożenie,
 - d) Skutki – jaki wpływ będzie miał zaistniały incydent na system informatyczny.
- 2) Podstawowe pojęcia:
 - a) **Zasoby/aktywa** - wszystkie elementy służące do przetwarzania, przechowywania, przekazywania informacji oraz zapewnienia im właściwego poziomu bezpieczeństwa, które podlegają w Starostwie ochronie:
 - Sprzęt teleinformatyczny służący przetwarzaniu danych;
 - Ludzie;
 - Aplikacje, w których są przetwarzane dane osobowe;
 - Pomieszczenia:
 - w których pracują osoby przetwarzające dane
 - gdzie są przechowywane dane osobowe
 - w których znajduje się sprzęt teleinformatyczny
 - Koszty dodatkowych zabezpieczeń oraz odbudowy systemu po incydencie,
 - b) **Prawdopodobieństwo** – zaistnienia, wystąpienia zagrożenia z uwagi na słabość zasobu,
 - c) **Skutek** - określa wysokość strat po zaistnieniu zagrożenia,
 - d) **Ryzyko** = iloczyn wartości skutków i prawdopodobieństwa wystąpienia zagrożenia.

Skala poziomu ryzyka 1-100

Wartość	Poziom ryzyka
1-10	Utrata bezpieczeństwa danych osobowych nie występuje
11-20	Niski poziom utraty bezpieczeństwa danych osobowych
21-50	Średni poziom utraty bezpieczeństwa danych osobowych
51-80	Wysoki poziom utraty bezpieczeństwa danych osobowych
81-100	Maksymalny poziom utraty bezpieczeństwa danych osobowych

Prawdopodobieństwo wystąpienia określonego zagrożenia dla systemu informatycznego

Wartość	Poziom
0-1	Brak , nieprawdopodobne
2-3	Niskie , może się zdarzyć, ale nie w ciągu roku
4-6	Średnie , może się zdarzyć w ciągu roku
7-8	Wysokie, może się wydarzyć w ciągu 6 miesięcy
9-10	B. wysokie, może się wydarzyć w ciągu 3 miesięcy

Skutki utraty zasobów dla atrybutu poufności

Wartość	Poziom ryzyka
1	Utrata poufności nie występuje
2-3	Niski skutek utraty poufności
4-6	Średni skutek utraty poufności
7-8	Wysoki skutek utraty poufności
9-10	Bezwzględny skutek utraty poufności

Skutki utraty zasobów dla atrybutu integralności

Wartość	Poziom ryzyka
1	Utrata integralności nie występuje
2-3	Niski skutek utraty integralności
4-6	Średni skutek utraty integralności
7-8	Wysoki skutek utraty integralności
9-10	Bezwzględny skutek utraty integralności

Skutki utraty zasobów dla atrybutu rozliczalności

Wartość	Poziom ryzyka
1	Utrata dostępności nie występuje
2-3	Niski skutek utraty rozliczalności
4-6	Średni skutek utraty rozliczalności
7-8	Wysoki skutek utraty rozliczalności
9-10	Bezwzględny skutek utraty rozliczalności

3) MACIERZ RYZYKA

Prawdopodobieństwo (P)	10	Bardzo wysokie	10	30	60	80	100
	8	Wysokie	8	24	48	64	80
	6	Średnie	6	18	36	48	60
	3	Niskie	3	9	18	24	30
	1	Brak	1	3	6	8	10
			Utrata nie występuje	Niski stopień utraty	Średni stopień utraty	Duży stopień utraty	Bardzo duży stopień utraty
			1	3	6	8	10
			Skutki (S)				

Reakcja na ryzyko:

brak akceptacji, ADO podejmuje decyzję
do decyzji ADO
akceptacja

STAROSTA ŁOWICKI

Krzysztof Figat

Załącznik nr 2
do Analizy zagrożeń i ryzyka
przetwarzania danych osobowych
w Starostwie Powiatowym w Łowiczu,
wprowadzonej Zarządzeniem Nr 40/2018
Starosty Łowickiego z dnia 23.05.2018r.
w sprawie wprowadzenia
Analizy zagrożeń
i ryzyka przetwarzania danych osobowych
w Starostwie Powiatowym w Łowiczu

Zagrożenia w obszarze przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu

- 1) Słabości kontroli zarządczej w zakresie ochrony danych osobowych.
- 2) Zagrożenia związane z bezpieczeństwem przetwarzania danych osobowych
- 3) Zagrożenie związane poufnością danych osobowych przetwarzanych w systemie informatycznym.
- 4) Zagrożenie związane z integralnością danych osobowych przetwarzanych w systemie informatycznym.
- 5) Zagrożenie związane z rozliczalnością danych osobowych przetwarzanych w systemie informatycznym.

STAROSTA ŁOWICKI

Krzysztof Figiel

Załącznik nr 3
do Analizy zagrożeń i ryzyka przetwarzania danych osobowych
w Starostwie Powiatowym w Łowiczu wprowadzonej Zarządzeniem Nr 10/2018
Starosty Łowickiego z dnia 23 maja 2018 r.
w sprawie wprowadzenia Analizy zagrożeń i ryzyka przetwarzania danych osobowych
w Starostwie Powiatowym w Łowiczu

MACIERZ SZACOWANIA RYZYKA DLA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W STAROSTWIE POWIATOWYM W ŁOWICZU

Zasoby	Szacowanie	Zagrożenia																		RAZEM (średnia)	
		Poufność						Rozliczalność						Integralność							
	S																				
	P																				
	Ryzyko																				
	S																				
	P																				
	Ryzyko																				
	S																				
	P																				
	Ryzyko																				
	S																				
	P																				
	Ryzyko																				
	S																				
	P																				
	Ryzyko																				
OGÓŁEM																					

STAROSTA ŁOWICKI

Krzysztof Figat

Załącznik nr 4
do Analizy zagrożeń i ryzyka
przetwarzania danych osobowych
w Starostwie Powiatowym w Łowiczu
wprowadzonej Zarządzeniem Nr 40/2018
Starosty Łowickiego z dnia 23 maja 2018 r.
w sprawie wprowadzenia Analizy zagrożeń
i ryzyka przetwarzania danych osobowych
w Starostwie Powiatowym w Łowiczu

SPRAWOZDANIE DLA ADMINISTRATORA DANYCH OSOBOWYCH

przygotowane na podstawie Analizy zagrożeń i ryzyka
przetwarzania danych osobowych w Starostwie Powiatowym w Łowiczu
przeprowadzonej w (dzień lub/i miesiąc rok)

STAROSTA ŁOWICKI

Krzysztof Figat

ID	ZAGROŻENIE	SKUTEK	REAKCJA	DZIAŁANIE	WŁAŚCICIEL RYZYKA	DECYZJA ADO

Wnioski:

Działania do podjęcia roku:

Łowicz, dnia

.....

.....

(podpis Inspektora)

(podpis ASI)

Akceptacja, dnia

(podpis Administratora)

STAROSTA ŁOWICKI

Krzysztof Figat