**ZARZĄDZENIE NR 395**

**WOJEWODY MAZOWIECKIEGO**

z dnia 30 października 2020 r.

**w sprawie polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie**

Na podstawie art. 69 ust. 1 pkt 3 i 68 ust. 2 pkt 7 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869, z późn. zm.[[1]](#footnote-1)1)) oraz art. 17 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2019 r. poz. 1464) zarządza się, co następuje:

**Rozdział 1**

**Postanowienia ogólne**

1. 1. Zarządzenie określa politykę zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie, która określa całościowe zasady i sposób funkcjonowania systemu zarządzania ryzykiem, w szczególności:
   1. rolę, zakres zadań i obowiązków uczestników systemu;
   2. zasady dokonywania identyfikacji, analizy i oceny ryzyka;
   3. zasady określania reakcji na ryzyko;
   4. zasady identyfikowania i raportowania incydentów;
   5. zakres i sposób monitorowania oraz raportowania ryzyka.

2. Ilekroć w niniejszym zarządzeniu jest mowa o:

1) **Urzędzie** – należy przez to rozumieć Mazowiecki Urząd Wojewódzki w Warszawie;

1. **Wojewodzie** – należy przez to rozumieć Wojewodę Mazowieckiego;
2. **akceptowalnym poziomie ryzyka** – należy przez to rozumieć ustalony poziom istotności ryzyka, przy którym nie jest wymagane podejmowanie działań zaradczych. Akceptowalny poziom ryzyka w Urzędzie ustalono na poziomie niskim;
3. **aktywach** – należy przez to rozumieć wszystko, co dla Urzędu ma wartość i, co dla jego dobra, należy chronić, aby Urząd funkcjonował w sposób niezakłócony;
4. **analizie ryzyka** – należy przez to rozumieć proces dążący do poznania charakteru i poziomu istotności ryzyka poprzez oszacowanie prawdopodobieństwa wystąpienia i siły oddziaływania, przy uwzględnieniu skuteczności istniejących mechanizmów kontrolnych, służący wypracowaniu decyzji, co do dalszego postępowania z ryzykiem;
5. **analizie ryzyka ilościowej** – należy przez to rozumieć analizę, w której stosuje się skalę o numerycznych wartościach (w przeciwieństwie do opisowych skali stosowanych w analizie jakościowej), zarówno dla następstw, jak i prawdopodobieństwa wystąpienia, wykorzystując dane z różnych źródeł;
6. **analizie ryzyka jakościowej** – należy przez to rozumieć analizę, w której stosuje się skalę atrybutów kwalifikujących do opisania wielkości potencjalnych następstw (np.: niski, średni i wysoki) oraz prawdopodobieństwa, że następstwa te mogą się urzeczywistnić;
7. **analizie ryzyka mieszanej** – należy przez to rozumieć analizę, w której wykorzystane są elementy analizy ilościowej i jakościowej;
8. **bezpieczeństwie informacji** – należy przez to rozumieć stan, gdy ryzyko naruszenia atrybutów bezpieczeństwa nie przekracza wartości akceptowalnych;
9. **celu** – należy przez to rozumieć zamierzony rezultat działalności, który ma być osiągnięty w określonym czasie, poprzez realizację programów, projektów, zadań, podzadań;
10. **czynniku ryzyka** – należy przez to rozumieć okoliczności, stan prawny, stan faktyczny, które mogą, ale nie muszą wywołać ryzyko wystąpienia niezgodności;
11. **dyrektorze** – należy przez to rozumieć dyrektora wydziału, biura, kierownika Zespołu Audytu Wewnętrznego, Komendanta Państwowej Straży Łowieckiej;
12. **EZD** – należy przez to rozumieć system Elektronicznego Zarządzania Dokumentacją funkcjonujący w Urzędzie;
13. **identyfikacji ryzyka** – należy przez to rozumieć proces wyszukiwania, rozpoznawania, analizowania i opisywania ryzyka;
14. **incydencie** – należy przez to rozumieć niepożądane zdarzenie o negatywnych skutkach dla bezpieczeństwa informacji w Urzędzie;
15. **incydencie bezpieczeństwa** – należy przez to rozumieć zdarzenie, które skutkuje zniszczeniem, utratą, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
16. **kierownictwu Urzędu** – należy przez to rozumieć Wojewodę, I i II Wicewojewodę oraz Dyrektora Generalnego Urzędu;
17. **komórce organizacyjnej** – należy przez to rozumieć wydział, biuro, Zespół Audytu Wewnętrznego, Państwową Straż Łowiecką;
18. **kryteriach oceny ryzyka** – należy przez to rozumieć poziomy odniesienia, względem których określa się ważność ryzyka dla realizacji celów i zadań; mogą pochodzić z przepisów prawa, norm, innych regulacji i wymogów;
19. **mechanizmach kontrolnych** – należy przez to rozumieć wszystkie czynniki, które modyfikują ryzyko, w tym: polityki, zarządzenia, procedury, instrukcje, praktyki, fizyczne i techniczne środki zabezpieczeń, systemy, zaprojektowane i wdrożone w celu ograniczenia prawdopodobieństwa wystąpienia ryzyka i/lub siły jego oddziaływania; podstawowy zestaw mechanizmów kontrolnych nie stanowi katalogu zamkniętego;
20. **mierniku realizacji celu** – należy przez to rozumieć wartościowe lub ilościowe określenie planowanego i wykonanego poziomu efektów z poniesionych nakładów;
21. **monitorowaniu ryzyka** – należy przez to rozumieć obserwowanie ocenionych ryzyk pod kątem zmiany siły oddziaływania i prawdopodobieństwa wystąpienia, adekwatności przyjętej reakcji na ryzyko oraz skuteczności funkcjonujących mechanizmów kontrolnych;
22. **ocenie ryzyka** – należy przez to rozumieć całościowy proces identyfikacji, analizy oraz ewaluacji ryzyka; porównanie wyników analizy ryzyka z kryteriami oceny ryzyka oraz poziomami istotności ryzyka w celu stwierdzenia czy ryzyko, jego istotność i charakter są akceptowalne. Ocena ryzyka wspomaga podejmowanie decyzji o sposobie reakcji na ryzyko i ustalanie priorytetów wdrażania postępowania z ryzykiem;
23. **odporności** – należy przez to rozumieć siłę oddziaływania mechanizmów kontrolnych na zidentyfikowane ryzyka;
24. **opisie ryzyka** – należy przez to rozumieć wskazanie źródeł i przyczyn powodujących powstanie ryzyka, zdarzeń i okoliczności jego wystąpienia lub zmiany oraz skutków i następstw wystąpienia ryzyka;
25. **pełnomocniku** – należy przez to rozumieć pełnomocnika Wojewody do spraw zarządzania ryzykiem;
26. **planie postępowania z ryzykiem** – należy przez to rozumieć plan postępowania z ryzykiem oszacowanym na poziomie bardzo wysokim;
27. **podatności** – należy przez to rozumieć słabość aktywu (zasobu) lub zabezpieczenia, która może być wykorzystana przez jedno lub więcej zagrożeń;
28. **poziomie ryzyka inherentnego** – należy przez to rozumieć wielkość ryzyka oszacowaną, jako iloczyn prawdopodobieństwa wystąpienia i siły oddziaływania ryzyka bez uwzględnienia siły stosowanych mechanizmów kontrolnych;
29. **poziomie ryzyka rezydualnego** – należy przez to rozumieć wielkość ryzyka oszacowaną, jako iloczyn prawdopodobieństwa wystąpienia i siły oddziaływania ryzyka z uwzględnieniem siły stosowanych mechanizmów kontrolnych;
30. **pracowniku** – należy przez to rozumieć osoby zatrudnione w Urzędzie, bez względu na podstawę stosunku pracy oraz osoby zatrudnione na podstawie umów cywilno-prawnych, a także stażystów, wolontariuszy;
31. **raporcie ryzyka** – należy przez to rozumieć roczną informację na temat wpływu ryzyk na realizację celów i zadań komórki organizacyjnej;
32. **raporcie ryzyka Urzędu** – należy przez to rozumieć roczną informację na temat wpływu ryzyk na realizację celów i zadań Urzędu w zakresie przekazywanym do pełnomocnika;
33. **raportowaniu ryzyka** – należy przez to rozumieć przekazywanie właściwym pracownikom Urzędu informacji o aktualnym stanie ryzyka i sposobie zarządzania ryzykiem;
34. **rejestrze ryzyka** – należy przez to rozumieć indywidualne zestawienie ryzyk komórek organizacyjnych, zawierające informacje o wyniku przeprowadzonej oceny ryzyka w stosunku do zaplanowanych do realizacji celów i zadań, a także wybranej reakcji na ryzyko;
35. **rejestrze ryzyka Urzędu** – należy przez to rozumieć zbiorcze zestawienie zawierające informacje o wyniku przeprowadzonej oceny ryzyka w Urzędzie w stosunku do zaplanowanych do realizacji celów i zadań, a także wybranej reakcji na ryzyko;
36. **ryzyku** – należy przez to rozumieć możliwość wystąpienia zdarzenia, działania lub zaniechania, które może wpłynąć na wykonywanie zadań bądź na zdolność Urzędu do realizacji celów jego działalności; a w przypadku bezpieczeństwa informacji – potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywa lub grupy aktywów, powodując w ten sposób naruszenie poufności, integralności, dostępności lub innych atrybutów bezpieczeństwa informacji;
37. **ryzyku projektu** – należy przez to rozumieć prawdopodobieństwo wystąpienia zjawiska lub działania, które może mieć pozytywne lub negatywne skutki dla przebiegu całego projektu lub/i jego poszczególnych części;
38. **ryzyku inherentnym** – należy przez to rozumieć ryzyko nieodłącznie związane z charakterem działalności, operacji i struktur zarządzania, które może być źródłem istotnych błędów lub nieprawidłowości; jest to ryzyko niepoddane działaniu żadnych mechanizmów kontrolnych, ani jakimkolwiek działaniom zaradczym mającym doprowadzić do jego ograniczenia lub likwidacji;
39. **ryzyku rezydualnym** – należy przez to rozumieć ryzyko po zastosowaniu mechanizmów kontrolnych, istniejące po podjęciu działań zaradczych mających doprowadzić do jego ograniczenia lub likwidacji;
40. **ryzyku strategicznym** – należy przez to rozumieć niepewność związaną ze zdarzeniem, działaniem lub zaniechaniem, które może wpłynąć na zdolność Urzędu do realizacji celów strategicznych;
41. **systemie zarządzania ryzykiem** – należy przez to rozumieć zestaw elementów/ czynników oraz skoordynowanych działań określonych w politykach, zarządzeniach, procedurach Urzędu, podejmowanych systematycznie w procesie kierowania i nadzoru nad realizacją celów;
42. **ustalaniu kontekstu** – należy przez to rozumieć analizę otoczenia, definiowanie zewnętrznych i wewnętrznych parametrów, które powinny być uwzględniane podczas zarządzania ryzykiem;
43. **WK** – należy przez to rozumieć Wydział Kontroli w Urzędzie;
44. **właścicielu celu** – należy przez to rozumieć członków kierownictwa i dyrektorów w Urzędzie odpowiedzialnych za realizację danego celu;
45. **właścicielu procesu** – należy przez to rozumieć członków kierownictwa i dyrektorów w Urzędzie odpowiedzialnych za nadzór i monitorowanie ryzyk w zakresie posiadanych uprawnień wynikających z regulaminu organizacyjnego Urzędu lub wewnętrznych regulaminów organizacyjnych;
46. **właścicielu ryzyka** – należy przez to rozumieć członków kierownictwa i dyrektorów w Urzędzie odpowiedzialnych za zarządzanie ryzykiem w ramach posiadanych uprawnień do podejmowania decyzji zarządczych; właścicielem ryzyka w Urzędzie jest dyrektor odpowiedzialny za realizację celu, do którego odnosi się ryzyko;
47. **właścicielu zasobu** – należy przez to rozumieć w szczególności członków kierownictwa i dyrektorów w Urzędzie, właścicieli ryzyka, administratora danych osobowych;
48. **zarządzaniu ryzykiem** – należy przez to rozumieć działania polegające na ocenie ryzyka, określeniu reakcji na ryzyko oraz monitorowaniu skuteczności podjętych decyzji dla zwiększenia prawdopodobieństwa realizacji celów;
49. **zasobie** – należy przez to rozumieć wszelkie aktywa, ludzi, umiejętności, technologie, obiekty oraz dostawy i informacje (w formie elektronicznej i innej), których dostępności Urząd potrzebuje w celu prowadzenia działalności i osiągnięcia celu;
50. **ZAW** – należy przez to rozumieć Zespół Audytu Wewnętrznego w Urzędzie.

**Rozdział 2**

**Polityka zarządzania ryzykiem w Urzędzie**

**§ 2.** 1. Zarządzanie ryzykiem stanowi istotny element systemu kontroli zarządczej Urzędu i jest oparte na istniejących źródłach informacji w Urzędzie.

1. System zarządzania ryzykiem jest dostosowany do specyfiki Urzędu, złożoności struktury organizacyjnej, zakresu delegowanych uprawnień i pełnomocnictw oraz realizowanych celów i zadań, a także obowiązków wynikających z przepisów prawa.
2. Poziom szczegółowości informacji gromadzonych w systemie jest dostosowany do złożoności struktury organizacyjnej i zapotrzebowania kierownictwa na poszczególnych poziomach zarządzania.
3. Proces zarządzania ryzykiem polega na systematycznym stosowaniu polityk, instrukcji i procedur opisujących ciąg zaplanowanych, wykonywanych i monitorowanych działań udokumentowanych w sposób określony w niniejszym zarządzeniu.
4. Kierownictwo Urzędu, dyrektorzy i pracownicy Urzędu są zaangażowani w rozwój systemu zarządzania ryzykiem poprzez:
5. wspieranie strategii, weryfikowanie założeń, projektów i zadań wspierających monitorowanie i doskonalenie funkcjonowania systemu zarządzania ryzykiem w Urzędzie;
6. wzmacnianie odporności Urzędu na pojawiające się zagrożenia, podejmowanie działań wyprzedzających, umożliwiających optymalne wykorzystanie zasobów oraz rozwój Urzędu.
7. W ramach systemu zarządzania ryzykiem działalność Urzędu ukierunkowana jest w szczególności na:
   1. realizację misji i wizji Urzędu w sposób oszczędny, efektywny i skuteczny;
   2. monitorowanie i ocenę stopnia realizacji celów w oparciu o mierniki realizacji zadań dla komórek organizacyjnych Urzędu;
   3. identyfikowanie, szacowanie poziomu ryzyka, analizę kluczowych czynników ryzyka i określenie reakcji na ryzyko, które może zakłócić lub uniemożliwić realizację celów;
   4. dokumentowanie czynności służących realizacji celów;
   5. zapewnienie zgodności z obowiązującymi regulacjami prawnymi, aktami wykonawczymi, standardami i normami;
   6. optymalizowanie realizowanych procesów oraz zarządzanie potencjalnymi szansami;
   7. kształtowanie pozytywnego wizerunku Urzędu.
8. Dyrektorzy oraz pracownicy Urzędu:
9. są uczestnikami procesu zarządzania ryzykiem z rolą dookreśloną w ramach opisów stanowisk pracy oraz zakresów odpowiedzialności w systemie zarządzania ryzykiem;
10. przekazują na właściwy poziom zarządzania informacje o ryzykach występujących i zagrażających realizacji wyznaczonych celów i zadań Urzędu;
11. są odpowiedzialni za realizację celów i zadań w sposób oszczędny, efektywny, skuteczny;
12. podnoszą swoje kwalifikacje w zakresie identyfikacji, analizy, oceny i zarządzania ryzykiem.
13. System zarządzania ryzykiem w Urzędzie podlega monitorowaniu, przeglądom oraz doskonaleniu.
14. Raportowanie ryzyka jest zintegrowane ze strukturą organizacyjną Urzędu.

**Rozdział 3**

**Cel zarządzania ryzykiem**

1. 1. Celem funkcjonowania systemu zarządzania ryzykiem w Urzędzie w szczególności jest:
2. zwiększenie prawdopodobieństwa osiągnięcia wyznaczonych celów i zadań w sposób oszczędny, efektywny i skuteczny poprzez ograniczanie zagrożeń i wykorzystywanie szans, a także poprawę standardów zarządzania w Urzędzie;
3. zidentyfikowanie ryzyk do celów i zadań w szczególności:
4. zawartych w planie działalności na dany rok,
5. w systemie ochrony danych osobowych,
6. w obszarze bezpieczeństwa informacji,
7. w obszarze informacji niejawnych i prawnie chronionych,
8. w obszarach narażonych na występowanie zagrożeń korupcyjnych.
9. Działania podejmowane w ramach systemu zarządzania ryzykiem są dokumentowane.
10. Zarządzanie ryzykiem w Urzędzie prowadzi się dla wszystkich istotnych obszarów i zasobów Urzędu.
11. System zarządzania ryzykiem w Urzędzie realizowany jest na czterech poziomach:
12. zarządzania strategicznego – realizowanego przy współudziale Kierownictwa Urzędu i pełnomocnika;
13. zarządzania operacyjnego – realizowanego przy współudziale dyrektorów;
14. koordynowania systemu zarządzania ryzykiem i monitoringu – realizowanego wspólnie przez WK i pełnomocnika oraz właścicieli zasobów, ryzyka, celu;
15. diagnozy stanu zarządzania ryzykiem – realizowanej przez WK wraz z pełnomocnikiem.

**Rozdział 4**

**Zakres zadań i obowiązków**

1. Do kompetencji kierownictwa Urzędu w zakresie zarządzania ryzykiem należy w szczególności:
2. zatwierdzanie strategii zarządzania ryzykiem w Urzędzie;
3. zarządzanie ryzykiem strategicznym;
4. podejmowanie decyzji, dokonywanie wyborów, ustalanie priorytetów działań z uwzględnieniem informacji otrzymywanych w ramach systemu raportowania;
5. ocena skuteczności systemu zarządzania ryzykiem;
6. zatwierdzanie raportu ryzyka Urzędu, rejestru ryzyka Urzędu oraz jego półrocznej aktualizacji;
7. wprowadzanie zmian w zasadach i trybie funkcjonowania systemu zarządzania ryzykiem w Urzędzie;
8. wdrożenie odpowiednich zabezpieczeń dla danych osobowych przetwarzanych w strukturach Urzędu, do czego koniecznym elementem jest wykonywanie analizy ryzyka;
9. zarządzanie ryzykami, o których mowa w § 3 ust. 1 pkt 2.
10. 1. Do zadań wspólnych WK i pełnomocnika należy w szczególności:
11. koordynowanie weryfikacji poprawności funkcjonowania systemu zarządzania ryzykiem w Urzędzie;
12. rekomendowanie Kierownictwu Urzędu kierunków rozwoju systemu zarządzania ryzykiem w Urzędzie i projektowanych zmian;
13. zapewnienie niezbędnej spójności w systemie zarządzania ryzykiem w Urzędzie;
14. upowszechnianie wiedzy, doskonalenie umiejętności i wspieranie działań na rzecz zwiększenia świadomości w zakresie zarządzania ryzykiem wśród uczestników systemu;
15. dokonywanie przeglądu skuteczności funkcjonowania systemu zarządzania ryzykiem w Urzędzie i projektowanie zmian;
16. organizowanie bieżącej współpracy z właścicielami ryzyka;
17. organizowanie współpracy, w tym wnioskowanie w uzgodnieniu z dyrektorami o  powołanie stałych lub zadaniowych zespołów, w celu wypracowania i testowania zasad, procedur i narzędzi w systemie zarządzania ryzykiem;
18. zapewnienie funkcjonowania systemu raportowania określonego w zarządzeniu;
19. prowadzenie rejestru ryzyka do planu działalności Urzędu na dany rok i jego półrocznej aktualizacji;
20. opracowanie raportu ryzyka Urzędu za rok poprzedzający dany rok;
21. prowadzenie rejestru ryzyka Urzędu w zakresie ryzyk związanych z nadużyciami i korupcją.

2. WK wraz z pełnomocnikiem koordynują działania w zakresie przepływu informacji dotyczących oceny istotnych ryzyk i zagrożeń oraz ich wpływu na realizację celów i zadań Urzędu współpracując w szczególności z:

* 1. ZAW w zakresie oceny systemu zarządzania ryzykiem w Urzędzie;
  2. Inspektorem Ochrony Danych/Zastępcą Inspektora Ochrony Danych w zakresie oceny bezpieczeństwa przetwarzania danych osobowych w Urzędzie;
  3. Biurem Informatyki i dyrektorami w zakresie bezpieczeństwa informacji;
  4. pełnomocnikiem do spraw polityki antykorupcyjnej w zakresie identyfikacji ryzyk związanych z nadużyciami, w tym korupcją;
  5. pełnomocnikiem do spraw ZSZJ w zakresie identyfikacji ryzyk związanych z auditami wewnętrznymi;
  6. pełnomocnikiem do spraw bezpieczeństwa cyberprzestrzeni w zakresie identyfikacji ryzyka związanego z cyberbezpieczeństwem;
  7. pełnomocnikiem do spraw transformacji procesowej w zakresie identyfikacji ryzyka w zarządzaniu przez cele.

3. W ramach systemu zarządzania ryzykiem w Urzędzie prowadzi się w szczególności następujące rejestry:

1) rejestr ryzyka do planu działalności – prowadzony przez WK;

2) rejestr ryzyka nadużyć i korupcji w Urzędzie – prowadzony przez pełnomocnika do spraw polityki antykorupcyjnej;

3) rejestr ryzyka w zakresie ochrony danych osobowych Urzędu – prowadzony przez Inspektora Ochrony Danych;

4) rejestr ryzyka, o którym mowa w Polityce Bezpieczeństwa Informacji w Urzędzie, prowadzony przez WK w porozumieniu z pełnomocnikiem, którego wzór stanowi załącznik nr 2.

4. Administratorzy informacji, o których mowa w Polityce Bezpieczeństwa Informacji w Urzędzie, są zobowiązani do przeprowadzenia identyfikacji ryzyka w szczególności według atrybutów: poufność, dostępność, integralność, autentyczność i niezaprzeczalność, niezawodność wraz z planem postępowania z ryzykiem w zakresie aktywów informacyjnych danej komórki organizacyjnej.

1. Dyrektorzy zarządzają oraz sprawują nadzór w zakresie zarządzania ryzykiem w kierowanych komórkach organizacyjnych.
2. Do zadań właścicieli ryzyka należy w szczególności:
3. ustalenie kontekstu prowadzonej działalności;
4. weryfikacja poziomu realizacji celów w oparciu o dobór odpowiednich mierników;
5. ocena ryzyk związanych z realizacją celów, za które odpowiadają w zakresie prowadzonej działalności;
6. określenie reakcji w odniesieniu do poszczególnych ryzyk i zaistniałych zagrożeń;
7. wdrażanie działań zaradczych w stosunku do zidentyfikowanych ryzyk;
8. wypełnianie określonych w zarządzeniu obowiązków w zakresie raportowania;
9. bieżąca współpraca z WK i pełnomocnikiem, w tym realizacja otrzymywanych rekomendacji;
10. gromadzenie i analiza informacji o incydentach oraz raportowanie informacji o istotnych incydentach;
11. identyfikowanie i wykorzystywanie szans na efektywną realizację celów i zadań;
12. monitorowanie poziomu ryzyka oraz skuteczności decyzji dotyczących sposobu postępowania z ryzykiem.
13. Dyrektorzy, jako właściciele procesów odpowiedzialni są za realizację czynności przetwarzania, o których mowa w Polityce Bezpieczeństwa Informacji w Urzędzie.
14. Właściciele zasobów (dyrektorzy) odpowiedzialni są za zachowanie w szczególności atrybutów: poufności, dostępności, integralności, autentyczności i niezaprzeczalności, niezawodności danych osobowych oraz odporności systemów i usług przetwarzania wykorzystywanych do realizacji procesów, o których mowa w Polityce Bezpieczeństwa Informacji w Urzędzie.
15. 1. Dyrektorzy wskazani w rejestrach ryzyka są obowiązani do bieżącego monitorowania poziomu ryzyk w nich ujętych w zakresie, w jakim występują one w obszarze realizowanych zadań w komórce organizacyjnej oraz informowania WK i pełnomocnika o:
16. zmaterializowaniu się ryzyka;
17. potencjalnych nowych ryzykach lub istotnych zmianach poziomu ryzyk zidentyfikowanych w rejestrach ryzyka;
18. zdarzeniach, które mogą negatywnie wpływać na realizację celów;
19. pojawiających się możliwościach wykorzystania szans.

2. Pracownicy są obowiązani do informowania przełożonych między innymi o ryzykach związanych z nieprawidłowościami i nadużyciami, w tym korupcji, które mogą stanowić naruszenie prawa lub negatywnie oddziaływać na realizację celów i zadań komórki organizacyjnej oraz postrzeganie Urzędu przez klientów.

3. O ile okoliczności, o których mowa w ust. 2, dotyczą bezpośredniego przełożonego, pracownik powiadamia, z pominięciem ustalonej drogi służbowej, stosownie do okoliczności: Wojewodę lub Dyrektora Generalnego Urzędu.

1. Rolę audytu wewnętrznego w procesie oceny zarządzania ryzykiem regulują odrębne przepisy.

**Rozdział 5**

**Wyznaczanie celów**

1. Zasady wyznaczania celów, ustanawiania mierników realizacji celów, a także zasady monitorowania stopnia realizacji celów określa regulacja dotycząca zasad funkcjonowania kontroli zarządczej w Urzędzie.

**Rozdział 6**

**Identyfikacja i ocena ryzyka**

1. 1. W terminie do dnia 31 października każdego roku dyrektorzy dokonują identyfikacji i oceny ryzyka, w odniesieniu do wszystkich celów wskazanych w planie działalności na następny rok i innych dokumentach oraz do innych celów wybranych do realizacji w następnym roku.

2. W przypadku zmiany celów, właściciele przeprowadzają ponowną identyfikację i ocenę ryzyka.

3. W przypadku istotnej zmiany warunków, w których funkcjonuje właściciel ryzyka, dokonuje się ponownej identyfikacji i oceny ryzyka.

1. Ocena ryzyka strategicznego i operacyjnego dokonywana jest również w przypadku istotnej zmiany warunków, w których funkcjonuje Urząd.
2. 1. Celem identyfikacji ryzyka jest stworzenie listy ryzyk opartych na zdarzeniach, które mogą przyśpieszać lub opóźniać osiągnięcie celów.

2. W ramach identyfikacji ryzyka wykorzystuje się między innymi:

1. wyniki monitorowania realizacji wyznaczonych celów;
2. sposób organizacji i zarządzania komórką organizacyjną;
3. jakość wewnętrznych i zewnętrznych regulacji prawnych;
4. uwarunkowania makroekonomiczne;
5. uwarunkowania społeczno-polityczne;
6. informacje o incydentach;
7. ustalenia z przeprowadzonych audytów i kontroli.

3. W ramach identyfikacji ryzyka rozważane są czynniki ryzyka, w szczególności zdarzenia, działania lub zaniechania, które mogą spowodować wystąpienie ryzyka lub też jego zwiększenie/zmniejszenie, wynikające ze źródeł zewnętrznych i wewnętrznych.

4. Wynik ustaleń, o których mowa w ust. 2 i 3, zawiera się w formie opisu ryzyka.

1. 1. Celem analizy ryzyka jest poznanie charakteru ryzyka oraz oszacowanie poziomu jego istotności.

2. Analizie podlegają zidentyfikowane ryzyka dla różnych obszarów działalności Urzędu.

3. Analiza ryzyka wymaga określenia:

1) prawdopodobieństwa wystąpienia i siły oddziaływania ryzyka inherentnego bez uwzględnienia siły mechanizmów kontrolnych wpływających na prawdopodobieństwo wystąpienia ryzyka i siłę oddziaływania;

2) prawdopodobieństwa wystąpienia i siły oddziaływania ryzyka rezydualnego z  uwzględnieniem siły mechanizmów kontrolnych wpływających na prawdopodobieństwo wystąpienia ryzyka i siłę oddziaływania.

1. 1. Każde zidentyfikowane ryzyko podlega oszacowaniu z uwzględnieniem jego znaczenia dla osiągnięcia założonych celów.

2. Każde ryzyko szacowane jest z uwzględnieniem prawdopodobieństwa wystąpienia i  siły jego oddziaływania przy uwzględnieniu adekwatności, skuteczności i  efektywności istniejących mechanizmów kontrolnych, poprzez określenie siły mechanizmów kontrolnych wpływających zarówno na prawdopodobieństwo wystąpienia ryzyka, jak i siłę oddziaływania.

3. Oszacowanie prawdopodobieństwa wystąpienia ryzyka inherentnego i siły jego oddziaływania polega na przypisaniu każdemu z ryzyk punktacji od 1 do 4, gdzie:

1. 1 oznacza prawdopodobieństwo i siłę oddziaływania – niskie;
2. 2 oznacza prawdopodobieństwo i siłę oddziaływania – średnie;
3. 3 oznacza prawdopodobieństwo i siłę oddziaływania – wysokie;
4. 4 oznacza prawdopodobieństwo i siłę oddziaływania – bardzo wysokie.

4. Oszacowanie siły mechanizmów kontrolnych wpływających na prawdopodobieństwo wystąpienia ryzyka i siłę jego oddziaływania lub na jeden z tych elementów, polega na przypisaniu stosowanym mechanizmom kontrolnym punktacji od 1 do 3, gdzie:

1. 1 oznacza, że wdrożone i stosowane mechanizmy kontrolne w pewnym stopniu mogą ograniczyć prawdopodobieństwo materializacji ryzyka i siłę jego oddziaływania lub jednego z tych elementów, nie wystąpiły okoliczności, co wpływa na zmniejszenie oszacowania prawdopodobieństwa wystąpienia ryzyka i siły jego oddziaływania lub jednego z tych elementów o 1 punkt;
2. 2 oznacza, że wdrożone i stosowane mechanizmy kontrolne powinny ograniczyć prawdopodobieństwo materializacji ryzyka i siłę jego oddziaływania lub jednego z tych elementów, nie wystąpiły okoliczności, co wpływa na zmniejszenie oszacowania prawdopodobieństwa wystąpienia ryzyka i siły jego oddziaływania lub jednego z tych elementów o 2 punkty;
3. 3 oznacza, że wdrożone i stosowane mechanizmy kontrolne ograniczają prawdopodobieństwo materializacji ryzyka i siłę jego oddziaływania lub jednego z tych elementów, nie wystąpiły okoliczności, co wpływa na zmniejszenie oszacowania prawdopodobieństwa wystąpienia ryzyka i siły jego oddziaływania lub jednego z tych elementów o 3 punkty.

5. Na podstawie przeprowadzonej identyfikacji i oceny ryzyk, w celu ustalenia ich ważności dla realizowanych celów i zadań, należy dokonać hierarchizacji ryzyk, co oznacza uporządkowanie ryzyk według kryterium ich znaczenia dla osiągnięcia założonych celów.

1. 1. Matryca ryzyka jest graficzną prezentacją wyników szacowania ryzyka i służy do ustalenia hierarchii ewentualnych działań mających na celu zmniejszenie istotności ryzyka, wzór matrycy ryzyka stanowi załącznik nr 1 do zarządzenia.

2. W celu przedstawienia istotności ryzyka ustalono 4 poziomy ryzyka:

1. poziom niski – kolor zielony – któremu odpowiada przedział zaszeregowania 1-3 – oznacza akceptowalny poziom ryzyka, zaplanowanie i wdrożenie działań zaradczych zależy od decyzji właściciela ryzyka;
2. poziom średni – kolor żółty – któremu odpowiada przedział zaszeregowania 4-6 – oznacza konieczność stałego monitorowania poziomu ryzyka oraz możliwość zaplanowania działań zaradczych do ewentualnego wdrożenia;
3. poziom wysoki – kolor pomarańczowy – któremu odpowiada przedział zaszeregowania 8-9 – oznacza wymóg stałego monitorowania poziomu ryzyka oraz konieczność zaplanowania działań zaradczych do ewentualnego wdrożenia;
4. poziom bardzo wysoki – kolor czerwony – któremu odpowiada przedział zaszeregowania 12-16 – oznacza nieakceptowalny poziom ryzyka oraz konieczność opracowania i wdrożenia w terminie uzgodnionym z WK i pełnomocnikiem planu postępowania z ryzykiem bardzo wysokim, który sporządzany jest według wzoru, stanowiącego załącznik nr 4.

3. Przyjmuje się, że ryzyka nieakceptowalne (bardzo wysokie) właściciel może zaakceptować w przypadku, gdy zastosowano wszystkie możliwe i dostępne mechanizmy kontrolne i brak jest możliwości sprowadzenia ryzyka do niższego poziomu.

4. Członkowie kierownictwa, właściciel ryzyka względu na charakter ryzyka mogą obniżyć poziom ryzyka do akceptowalnego za pomocą odpowiednich mechanizmów kontrolnych.

1. Wyniki oceny ryzyka mają na celu stwierdzenie czy ryzyko, jego istotność i charakter są akceptowalne. Ocena ryzyka wspomaga podejmowanie decyzji o sposobie reakcji na ryzyko.

**Rozdział 7**

**Reakcja na ryzyko**

1. 1. Dla każdego zidentyfikowanego, poddanego analizie i ocenie ryzyka, jego właściciel wskazuje jedną z poniższych reakcji:
2. akceptacja – oznacza, że nie podejmuje się żadnych działań zaradczych, ale rozumie ewentualne skutki zdarzenia i świadomie godzi się na nie (np.: możliwość przeciwdziałania jest ograniczona lub koszt przeciwdziałania przewyższa potencjalne korzyści);
3. dzielenie się – częściowe lub całkowite przeniesienie ryzyka na inny podmiot;
4. unikanie – niepodejmowanie lub zaprzestanie działania narażającego na ryzyko (rezygnacja z realizacji celu);
5. ograniczanie – podjęcie działań zaradczych, które doprowadzić mają do likwidacji lub ograniczenia ryzyka.

2. Decyzję w zakresie zastosowanej reakcji na ryzyko podejmuje się z uwzględnieniem potencjalnych kosztów, które wiążą się z jego ograniczaniem, oraz potencjalnych korzyści, które wynikają z tego działania.

3. Przy wskazaniu reakcji na ryzyko należy uwzględnić określony w niniejszym zarządzeniu akceptowalny poziom ryzyka.

4. Właściciel ryzyka zobowiązany jest do monitorowania poziomu ryzyka i skuteczności decyzji dotyczących sposobu postępowania z ryzykiem. Monitorowanie dotyczy również zmian czynników zewnętrznych i wewnętrznych, które mogą generować nowe ryzyka i zmieniać istotność lub charakter istniejących.

5. Stosowane w Urzędzie podstawowe mechanizmy kontrolne, w szczególności zasady, oraz reakcje na zidentyfikowane ryzyko dotyczące bezpieczeństwa informacji określone są w Polityce Bezpieczeństwa Informacji w Urzędzie.

6. W stosunku do ryzyka oszacowanego na poziomie bardzo wysokim należy przeprowadzić szczegółową analizę oraz sporządzić plan postępowania z ryzykiem bardzo wysokim i podjąć jedną z niżej określonych decyzji:

1. rezygnacja z realizacji celu – wycofanie się z działań zagrożonych ryzykiem;
2. przesunięcie w czasie realizacji celu – wskazanie nowej daty osiągnięcia zakładanych rezultatów;
3. realizacja celu w ograniczonym zakresie – zmniejszenie zaplanowanych rezultatów działań;
4. wdrożenie działań sprowadzających ryzyko do akceptowalnego poziomu wraz ze wskazaniem osoby odpowiedzialnej za realizację opisanych działań;
5. realizacja celu przy akceptacji ryzyka na poziomie bardzo wysokim – brak dodatkowych działań zmniejszających ryzyko.

7. Plan postępowania z ryzykiem sporządza i podpisuje certyfikowanym podpisem elektronicznym właściciel ryzyka niezwłocznie po zidentyfikowaniu ryzyka bardzo wysokiego.

8. W przypadku ryzyk, o których mowa w ust. 6, dotyczących bezpieczeństwa informacji, decyzję w szczególności w zakresie identyfikacji analizy i oceny ryzyk oraz stosowanych zabezpieczeń podejmują członkowie Zespołu do spraw Systemu Zarządzania Bezpieczeństwem Informacji, w przypadku pozostałych – członkowie kierownictwa Urzędu i dyrektorzy.

9. Plan, o którym mowa w ust. 7, należy przekazać do WK i udostępnić pełnomocnikowi.

**Rozdział 8**

**Raportowanie o ryzykach**

1. W terminie do 31 października każdego roku dyrektorzy przekazują do WK i innych komórek organizacyjnych zgodnie z właściwością odpowiedzialnych za prowadzenie rejestrów ryzyk, o których mowa w § 6 ust. 3, oraz udostępniają pełnomocnikowi rejestry ryzyka wypełnione w zakresie komórki organizacyjnej zawierające informacje o:
2. ryzykach związanych z realizacją celów z planu działalności na następny rok;
3. wszystkich ryzykach do pozostałych celów i zadań, o których mowa w § 3 ust. 1 pkt 2, o istotności większej niż niskie.
4. 1. W terminie do dnia 15 lipca każdego roku dyrektorzy, przekazują do WK i innych komórek organizacyjnych zgodnie z właściwością odpowiedzialnych za prowadzenie rejestrów ryzyk, o których mowa w § 6 ust. 3, oraz udostępniają pełnomocnikowi półroczną aktualizację ryzyk, o których mowa w § 22 dla komórki organizacyjnej.

2. Na podstawie nadesłanych informacji WK dokonuje aktualizacji rejestrów ryzyka.

3. W ramach półrocznej aktualizacji rejestru ryzyka dyrektorzy, zobowiązani są do przeprowadzenia ponownej oceny ryzyk zidentyfikowanych w odniesieniu do wszystkich przypisanych im celów, a także innych celów realizowanych w danym roku oraz przekazania informacji o:

1. celach realizowanych przy ryzykach wysokich i bardzo wysokich;
2. celach zagrożonych - celach, dla których osiągnięta wartość miernika wskazuje, że realizacja na zaplanowanym poziomie może być niemożliwa do osiągnięcia w danym roku;
3. konsekwencjach niezrealizowania celów, o których mowa w pkt 2;
4. stopniu realizacji celów, w szczególności, o których mowa w pkt 1 i 2, poprzez wykazanie wartości wykonanego miernika według stanu na dzień 30 czerwca danego roku.
5. 1. W terminie do 31 stycznia każdego roku dyrektorzy przekazują WK i innych komórek organizacyjnych zgodnie z właściwością odpowiedzialnych za prowadzenie rejestrów ryzyk, o których mowa w § 6 ust. 3, oraz udostępniają pełnomocnikowi raporty ryzyka za zakończony rok dla komórki organizacyjnej w obszarach, o których mowa w § 22.

2. W raporcie ryzyka, o którym mowa w ust. 1, dyrektorzy przekazują także informację o pozostałych celach nieujętych w planie działalności, które nie były obarczone ryzykiem wysokim i bardzo wysokim, a mimo wszystko nie zostały zrealizowane na zaplanowanym poziomie. Dodatkowo należy wskazać przyczyny i konsekwencje braku realizacji tych celów.

1. 1. W przypadku zmian organizacyjnych, a w szczególności utworzenia, połączenia lub podziału komórek organizacyjnych, ich dyrektorzy w terminie 30 dni od utworzenia, połączenia lub podziału:
2. sporządzają i przekazują do WK oraz udostępniają pełnomocnikowi rejestr ryzyka, w którym dokonują wyboru celów realizowanych do końca danego roku, oceny ryzyk w odniesieniu do celów, wraz ze wskazaniem reakcji na ryzyko;
3. przekazują do WK i udostępniają pełnomocnikowi informację o ryzykach, których istotność osiągnęła poziom wysoki i bardzo wysoki.

2. W przypadku likwidacji komórki organizacyjnej, w ostatnim dniu jej funkcjonowania dyrektor przekazuje dyrektorowi WK i udostępnia pełnomocnikowi raport ryzyka według stanu na dzień likwidacji.

1. 1. W oparciu o otrzymane informacje WK wraz z pełnomocnikiem, w terminie 14 dni roboczych od dnia otrzymania ze wszystkich komórek organizacyjnych poprawnych informacji sporządza:
2. rejestr ryzyka Urzędu;
3. półroczną aktualizację rejestru ryzyka Urzędu na dany rok;
4. raport ryzyka Urzędu za zakończony rok.

2. Dokumenty, o których mowa w ust. 1, są sporządzane z uwzględnieniem poziomów zarządzania w Urzędzie.

1. 1. Wszystkie informacje i raporty w ramach systemu zarządzania ryzykiem przekazywane lub udostępniane w systemie EZD do WK lub pełnomocnika podpisywane są certyfikowanym podpisem elektronicznym.

2. Rejestr ryzyka, jego półroczna aktualizacja, raport ryzyka oraz informacja o zagrożeniach przekazywane do WK i udostępniane pełnomocnikowi w formie elektronicznej, stanowią pliki w formacie akceptowanym przez MS Excel, które należy przesyłać w systemie EZD.

3. Raportowanie ryzyka odbywa się w oparciu o procesy, obszary i funkcje określone w regulaminie organizacyjnym Urzędu.

**Rozdział 9**

**Raportowanie o ryzyku w obszarze przetwarzania danych osobowych**

1. 1. Trzy razy do roku dyrektorzy mają obowiązek przekazania Inspektorowi Ochrony Danych wypełnioną tabelę zawierającej informacje o występujących w komórkach organizacyjnych ryzykach związanych z przetwarzaniem danych osobowych. Informacje te są niezbędne do oszacowania bezpieczeństwa dla danych osobowych przetwarzanych w Urzędzie, wzór tabeli stanowi załącznik nr 3.

2. Informacje, o których mowa w ust. 1, umożliwią Inspektorowi Ochrony Danych przygotowanie działań mających na celu poprawę bezpieczeństwa przetwarzania danych osobowych w Urzędzie.

2. Tabele podpisane certyfikowanym podpisem elektronicznym przez dyrektora należy przesyłać w systemie EZD do Inspektora Ochrony Danych.

3. Dyrektorzy przekazują wypełnione tabele w terminach:

1) do dnia 31 października każdego roku na następny rok;

2) do dnia 15 lipca każdego roku za I półrocze roku bieżącego;

3) do dnia 31 stycznia każdego roku za rok poprzedni.

4. W oparciu o otrzymane informacje Inspektor Ochrony Danych, w terminie 14 dni roboczych od dnia otrzymania ze wszystkich komórek organizacyjnych poprawnych informacji, sporządza i udostępnia pełnomocnikowi oraz WK informacje w zakresie zidentyfikowanych ryzyk w obszarze przetwarzania danych osobowych oraz ich analizę.

5. Inspektor Ochrony Danych prowadzi rejestr ryzyka ochrony danych osobowych Urzędu oraz dokonuje półrocznej aktualizacji rejestru na podstawie uzyskanych informacji o zidentyfikowanych ryzykach.

6. Raport dotyczący identyfikacji i szacowania ryzyka w obszarze ochrony danych osobowych Urzędu za zakończony rok wraz z analizą jest przekazywany do wiadomości Dyrektorowi Generalnemu Urzędu oraz Zespołowi do spraw Systemu Zarządzania Bezpieczeństwem Informacji.

**Rozdział 10**

**Aplikacja wspierająca proces zarządzania ryzykiem w Urzędu**

1. Rejestr ryzyka, jego bieżąca oraz półroczna aktualizacja, raport ryzyka, w zakresie działalności komórek organizacyjnych są rejestrowane w formie elektronicznej wspierającej proces zarządzania ryzykiem w Urzędzie.

**Rozdział 11**

**Postanowienia końcowe**

1. 1. Działania podejmowane w ramach systemu zarządzania ryzykiem są uwzględniane w wewnętrznych regulaminach organizacyjnych komórek organizacyjnych.

2. Regulacje, o których mowa w ust. 1, powinny zawierać, co najmniej wskazanie:

1. zadań z zakresu zarządzania ryzykiem wraz z ich przypisaniem do wewnętrznych komórek organizacyjnych i osób pełniących określone funkcje oraz zakresu odpowiedzialności za bieżące zarządzanie ryzykiem;
2. procedury dotyczącej przepływu informacji do właściciela ryzyka stanowiące wewnętrzny system raportowania;
3. obowiązku rejestrowania ryzyka, jego oceny, monitorowania, dokumentowania i raportowania.
4. Nadzór nad wykonaniem zarządzenia powierza się Dyrektorowi Generalnemu Urzędu i Dyrektorowi WK.
5. Do dnia 31 grudnia 2020 r. komórki organizacyjne prowadzące właściwe rejestry lub metodyki są obowiązane dostosować je do wymagań określonych przepisami niniejszego zarządzenia.
6. Zarządzenie wchodzi w życie z dniem podpisania.

WOJEWODA MAZOWIECKI

KONSTANTY RADZIWIŁŁ

Załączniki do zarządzenia nr ……

Wojewody Mazowieckiego z dnia …………………………………

Załącznik nr 1

**Matryca ryzyka**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Prawdopodobieństwo wystąpienia** | |  |  |  |  |  |
| **Bardzo Wysokie** | **4** | **4** | **8** | **12** | **16** |  |
| **Wysokie** | **3** | **3** | **6** | **9** | **12** |  |
| **Średnie** | **2** | **2** | **4** | **6** | **8** |  |
| **Niskie** | **1** | **1** | **2** | **3** | **4** |  |
| Prawdopodobieństwo .  Wpływ …… | | **1** | **2** | **3** | **4** |  |
| **Niski** | **Średni** | **Wysoki** | **Bardzo Wysoki** | **wpływ/ siła oddziaływania** |
|  |  |  |  |  |  |  |
| **Legenda** |  |  |  |  |  |  |
| kolor: | | zielony | żółty | pomarańczowy | czerwony |  |
| przedział zaszeregowania: | | 1-3 | 4-6 | 8-9 | 12-16 |  |
| poziom ryzyka: | | **Niski** | **Średni** | **Wysoki** | **Bardzo Wysoki (nieakceptowalny)** |  |
|  |  |  |  |  |  |  |

Załącznik nr 2



Załącznik nr 3



Załącznik nr 4

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Plan postępowania z ryzykiem bardzo wysokim** | | | | | | | | | |
|  |  |  |  |  |  |  |  | Stan na dzień ………… r. | |
| **Lp.** | **Ryzyko** | **Dział lub proces** | **Dotyczy zagrożenia** | **Opis postępowania** | **Osoba odpowiedzialna za realizację** | **Planowane koszty realizacji** | **Planowana data zakończenia realizacji** | **Data zakończenia realizacji** | **Skuteczność (wg skali 1-4)** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

1. 1) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz.U. z 2019 r. poz. 1622, 1649 i 2020 oraz z 2020 r. poz. 284, 374, 568, 695 i 1175. [↑](#footnote-ref-1)