ZARZĄDZENIE
WOJEWODY MAZOWIECKIEGO

z dnia 01 kwietnia 2025 r.

w sprawie określenia 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 2024 r. poz. 1530, z późn. zm.[1)]) oraz art. 17 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2023 r. poz. 190 oraz z 2024 r. poz. 1907) zarządza się, co następuje:

Rozdział 1

Postanowienia ogólne

§ 1. 1. Zarządzenie określa politykę zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie, w tym całościowe zasady i sposób funkcjonowania systemu zarządzania ryzykiem, a w szczególności:

1) rolę, zakres zadań i obowiązków uczestników systemu zarządzania ryzykiem;
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 zarządzeniu jest mowa o:

1) **Urzędzie** – należy przez to rozumieć Mazowiecki Urząd Wojewódzki w Warszawie;
2) **Wojewodzie** – należy przez to rozumieć Wojewodę Mazowieckiego;
3) **akceptowalnym poziomie ryzyka** – należy przez to rozumieć ustalony poziom istotności ryzyka, przy którym nie jest wymagane podejmowanie działań zaradczych, który w Urzędzie ustalono na poziomie niskim;
4) **aktywach** – należy przez to rozumieć wszystko, co dla Urzędu ma wartość i, co dla jego dobra, należy chronić, aby Urząd funkcjonował w sposób niezakłócony;
5) **analizie ryzyka** – należy przez to rozumieć proces dążący do poznania charakteru i poziomu istotności ryzyka poprzez oszacowanie prawdopodobieństwa

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz.U. z 2024 r. poz. 1572, 1717, 1756 i 1907 oraz z 2025 r. poz. 39.

wystąpienia i siły oddziaływania, przy uwzględnieniu skuteczności istniejących mechanizmów kontrolnych, służący wypracowaniu decyzji, co do dalszego postępowania z ryzykiem;

6) **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;
7) **analizie ryzyka jakościowej** – należy przez to rozumieć analizę, w której stosuje się skalę atrybutów kwalifikujących do opisania wielkości potencjalnych następstw, posługując się określeniami: niski, średni, wysoki i bardzo wysoki oraz prawdopodobieństwa, że następstwa te mogą się urzeczywistnić;
8) **analizie ryzyka mieszanej** – należy przez to rozumieć analizę, w której wykorzystane są elementy analizy ilościowej i jakościowej;
9) **AW** – należy przez to rozumieć Zespół Audytu Wewnętrznego Urzędu.
10) **bezpieczeństwie informacji** – należy przez to rozumieć stan, gdy ryzyko naruszenia atrybutów bezpieczeństwa nie przekracza wartości akceptowalnych;
11) **celu** – należy przez to rozumieć zamierzony rezultat działalności, który ma być osiągnięty w określonym czasie, poprzez realizację programów, projektów, zadań, podzadań;
12) **członkach kierownictwa** – należy przez to rozumieć Wojewodę, I i II Wicewojewodę Mazowieckiego oraz Dyrektora Generalnego Urzędu;
13) **czynniku ryzyka** – należy przez to rozumieć okoliczności, stan prawny, stan faktyczny, które mogą, ale nie muszą wywołać ryzyko wystąpienia niezgodności;
14) **dyrektorze** – należy przez to rozumieć dyrektora wydziału, biura, kierownika AW, Komendanta Wojewódzkiego Państwowej Straży Łowieckiej, Mazowieckiego Wojewódzkiego Inspektora Nadzoru Geodezyjnego i Kartograficznego w Urzędzie;
15) **EZD** – należy przez to rozumieć system Elektronicznego Zarządzania Dokumentacją funkcjonujący w Urzędzie;
16) **identyfikacji ryzyka** – należy przez to rozumieć proces wyszukiwania, rozpoznawania, analizowania i opisywania ryzyka;
17) **incydencie** – należy przez to rozumieć niepożądane zdarzenie o negatywnych skutkach dla bezpieczeństwa informacji w Urzędzie;

18) **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;
19) **KOKZ** – należy przez to rozumieć komórkę organizacyjną koordynującą kontrolę zarządczą w Urzędzie;
20) **komórce organizacyjnej** – należy przez to rozumieć wydział, biuro, AW, Państwową Straż Łowiecką, Wojewódzką Inspekcję Geodezyjną i Kartograficzną w Urzędzie;
21) **koordynatorze** – należy przez to rozumieć koordynatora lub zastępcę koordynatora do spraw kontroli zarządczej i zarządzania ryzykiem w komórce organizacyjnej Urzędu, powołanego na mocy odrębnego zarządzenia;
22) **kryteriach oceny ryzyka** – należy przez to rozumieć poziomy odniesienia, względem których określa się ważność ryzyka dla realizacji celów i zadań, przy czym mogą one pochodzić z przepisów prawa, norm, innych regulacji i wymogów;
23) **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 siły jego oddziaływania, ocenianych według kryteriów: adekwatności, skuteczności, efektywności;
24) **mierniku realizacji celu** – należy przez to rozumieć wartościowe lub ilościowe określenie planowanego i wykonanego poziomu efektów z poniesionych nakładów;
25) **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;
26) **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, wspomagający podejmowanie decyzji

o sposobie reakcji na ryzyko i ustalanie priorytetów wdrażania postępowania z ryzykiem;

27) **odporności** – należy przez to rozumieć siłę oddziaływania mechanizmów kontrolnych na zidentyfikowane ryzyka;
28) **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;
29) **pełnomocniku** – należy przez to rozumieć pełnomocnika Wojewody do spraw zarządzania ryzykiem;
30) **planie postępowania z ryzykiem** – należy przez to rozumieć plan postępowania z ryzykiem rezydualnym oszacowanym na poziomie bardzo wysokim;
31) **podatności** – należy przez to rozumieć słabość aktywu, zasobu lub zabezpieczenia, która może być wykorzystana przez jedno lub więcej zagrożeń;
32) **poziomie ryzyka inherentnego** – należy przez to rozumieć wielkość ryzyka oszacowaną, jako iloczyn prawdopodobieństwa wystąpienia i siły oddziaływania ryzyka bez uwzględnienia siły stosowanych mechanizmów kontrolnych;
33) **poziomie ryzyka rezydualnego** – należy przez to rozumieć wielkość ryzyka oszacowaną, jako iloczyn prawdopodobieństwa wystąpienia i siły oddziaływania ryzyka z uwzględnieniem siły stosowanych mechanizmów kontrolnych;
34) **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, praktykantów, wolontariuszy;
35) **raporcie ryzyka** – należy przez to rozumieć roczną informację na temat wpływu ryzyk na realizację celów i zadań komórki organizacyjnej;
36) **raporcie ryzyka Urzędu** – należy przez to rozumieć roczną informację na temat wpływu ryzyk na realizację celów i zadań Urzędu w zakresie przekazywanym do pełnomocnika;
37) **raportowaniu ryzyka** – należy przez to rozumieć przekazywanie właściwym pracownikom Urzędu informacji o aktualnym stanie ryzyka i sposobie zarządzania ryzykiem;
38) **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;

39) **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;
40) **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;
41) **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;
42) **ryzyku inherentnym** – należy przez to rozumieć ryzyko nieodłączne związane z charakterem działalności, operacji i struktur zarządzania, które może być źródłem istotnych błędów lub nieprawidłowości, niepoddanym działaniu żadnych mechanizmów kontrolnych, ani jakimkolwiek działaniom zaradczym mającym doprowadzić do jego ograniczenia lub likwidacji;
43) **ryzyku rezydualnym** – należy przez to rozumieć ryzyko po zastosowaniu mechanizmów kontrolnych, istniejące po podjęciu działań zaradczych mających doprowadzić do jego ograniczenia lub likwidacji;
44) **ryzyku strategicznym** – należy przez to rozumieć niepewność związaną ze zdarzeniem, działaniem lub zaniechaniem, które może wpłynąć na zdolność Urzędu do realizacji celów strategicznych;
45) **systemie zarządzania ryzykiem** – należy przez to rozumieć zestaw elementów i czynników oraz skoordynowanych działań określonych w politykach, zarządzeniach, procedurach Urzędu, podejmowanych systematycznie w procesie kierowania i nadzoru nad realizacją celów;
46) **ustalaniu kontekstu** – należy przez to rozumieć analizę otoczenia, definiowanie zewnętrznych i wewnętrznych parametrów, które powinny być uwzględniane podczas zarządzania ryzykiem;
47) **właścicielu celu** – należy przez to rozumieć członków kierownictwa i dyrektorów w Urzędzie odpowiedzialnych za realizację danego celu;

48) **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;
49) **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;
50) **właścicielu zasobu** – należy przez to rozumieć w szczególności członków kierownictwa i dyrektorów w Urzędzie, właścicieli ryzyka, administratora danych osobowych;
51) **zarządzaniu ryzykiem** – należy przez to rozumieć proces identyfikacji, oceny i przeciwdziałania ryzyku, który obejmuje monitorowanie ryzyka i środków podejmowanych w celu jego ograniczania;
52) **zasobie** – należy przez to rozumieć wszelkie aktywa, ludzi, umiejętności, technologie, obiekty oraz dostawy i informacje w postaci elektronicznej i innej, których dostępności Urząd potrzebuje w celu prowadzenia działalności i osiągnięcia celu.

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.
2. 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.
3. Poziom szczegółowości informacji gromadzonych w systemie jest dostosowany do złożoności struktury organizacyjnej i zapotrzebowania kierownictwa na poszczególnych poziomach zarządzania.

4. Proces zarządzania ryzykiem polega na systematycznym stosowaniu polityk, instrukcji i procedur opisujących ciąg zaplanowanych, wykonywanych i monitorowanych działań udokumentowanych w sposób określony w zarządzeniu.
5. Członkowie kierownictwa, dyrektorzy i pracownicy Urzędu są zaangażowani w rozwój systemu zarządzania ryzykiem poprzez:
   1) wspieranie strategii, weryfikowanie założeń, projektów i zadań wspierających monitorowanie i doskonalenie funkcjonowania systemu zarządzania ryzykiem w Urzędzie;
   2) wzmacnianie odporności Urzędu na pojawiające się zagrożenia, podejmowanie działań wyprzedzających, umożliwiających optymalne wykorzystanie zasobów oraz rozwój Urzędu.
6. W ramach systemu zarządzania ryzykiem działalność Urzędu ukierunkowana jest w szczególności na:
   1) realizację misji 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.
7. Dyrektorzy oraz pracownicy Urzędu:
   1) są uczestnikami procesu zarządzania ryzykiem z rolą dookreśloną w ramach opisów stanowisk pracy oraz zakresów odpowiedzialności w systemie zarządzania ryzykiem;
   2) przekazują na właściwy poziom zarządzania informacje o ryzykach występujących i zagrażających realizacji wyznaczonych celów i zadań Urzędu;
   3) są odpowiedzialni za realizację celów i zadań w sposób oszczędny, efektywny, skuteczny;

4) podnoszą swoje kwalifikacje w zakresie identyfikacji, analizy, oceny i zarządzania ryzykiem.

8. System zarządzania ryzykiem w Urzędzie podlega monitorowaniu, przeglądom oraz doskonaleniu.
9. Raportowanie ryzyka jest zintegrowane ze strukturą organizacyjną Urzędu.

Rozdział 3

Cel zarządzania ryzykiem

§ 3. 1. Celem funkcjonowania systemu zarządzania ryzykiem w Urzędzie jest w szczególności:

1) 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;
2) zidentyfikowanie ryzyk do celów i zadań w szczególności:
   a) zawartych w planie działalności Urzędu na dany rok,
   b) w obszarze inwestycji,
   c) w systemie ochrony danych osobowych,
   d) w obszarze bezpieczeństwa informacji,
   e) w obszarze informacji niejawnych i prawnie chronionych,
   f) w obszarach narażonych na występowanie zagrożeń korupcyjnych,
   g) w obszarze ciągłości działania.

2. Działania podejmowane w ramach systemu zarządzania ryzykiem są dokumentowane.
3. Zarządzanie ryzykiem w Urzędzie prowadzi się dla wszystkich istotnych obszarów i zasobów Urzędu.

§ 4. System zarządzania ryzykiem w Urzędzie realizowany jest na czterech poziomach:

1) zarządzania strategicznego – realizowanego przy współudziale członków kierownictwa i pełnomocnika;
2) zarządzania operacyjnego – realizowanego przy współudziale dyrektorów;
3) koordynowania systemu zarządzania ryzykiem i monitoringu – realizowanego wspólnie przez KOKZ i pełnomocnika oraz koordynatorów i właścicieli zasobów, ryzyk i celów;
4) diagnozy stanu kontroli zarządczej, sporządzanej przez KOKZ przy udziale pełnomocnika.

Rozdział 4

Zakres zadań i obowiązków

§ 5. Do kompetencji członków kierownictwa w zakresie zarządzania ryzykiem należy w szczególności:

1) zatwierdzanie strategii zarządzania ryzykiem w Urzędzie;
2) zarządzanie ryzykiem strategicznym;
3) podejmowanie decyzji, dokonywanie wyborów, ustalanie priorytetów działań z uwzględnieniem informacji otrzymywanych w ramach systemu raportowania;
4) ocena skuteczności systemu zarządzania ryzykiem;
5) zatwierdzanie raportu ryzyka Urzędu i rejestru ryzyka Urzędu;
6) wprowadzanie zmian w zasadach i trybie funkcjonowania systemu zarządzania ryzykiem w Urzędzie;
7) wdrożenie odpowiednich zabezpieczeń dla danych osobowych przetwarzanych w strukturach Urzędu, do czego koniecznym elementem jest wykonywanie analizy ryzyka;
8) zarządzanie ryzykami, o których mowa w § 3 w ust. 1 w pkt 2.

§ 6. 1. Do zadań wspólnych KOKZ i pełnomocnika należy w szczególności:

1) koordynowanie weryfikacji poprawności funkcjonowania systemu zarządzania ryzykiem w Urzędzie;
2) rekomendowanie członkom kierownictwa kierunków rozwoju systemu zarządzania ryzykiem w Urzędzie i projektowanych zmian;
3) zapewnienie niezbędnej spójności w systemie zarządzania ryzykiem w Urzędzie;
4) upowszechnianie wiedzy, doskonalenie umiejętności i wspieranie działań na rzecz zwiększenia świadomości w zakresie zarządzania ryzykiem wśród uczestników systemu zarządzania ryzykiem;
5) dokonywanie przeglądu skuteczności funkcjonowania systemu zarządzania ryzykiem w Urzędzie i projektowanie zmian;
6) organizowanie bieżącej współpracy z właścicielami ryzyka;
7) 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;
8) zapewnienie funkcjonowania systemu raportowania określonego w zarządzeniu;

9) prowadzenie rejestru ryzyka do planu działalności Urzędu na dany rok i jego aktualizacji;
10) opracowanie raportu ryzyka Urzędu za rok poprzedzający dany rok;
11) prowadzenie rejestru ryzyka Urzędu w zakresie ryzyk związanych z nadużyciami i korupcją.

2. KOKZ przy udziale pełnomocnika koordynuje 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) AW w zakresie oceny systemu zarządzania ryzykiem w Urzędzie;
   2) Wydziałem Kontroli w zakresie ryzyk wynikających z wyników przeprowadzonych kontroli w Urzędzie;
   3) Inspektorem Ochrony Danych lub zastępcą Inspektora Ochrony Danych w zakresie oceny bezpieczeństwa przetwarzania danych osobowych w Urzędzie;
   4) pełnomocnikiem do spraw bezpieczeństwa informacji w Urzędzie i dyrektorami w zakresie bezpieczeństwa informacji;
   5) pełnomocnikiem do spraw polityki antykorupcyjnej w zakresie identyfikacji ryzyk związanych z nadużyciami, w tym korupcji;
   6) pełnomocnikiem do spraw bezpieczeństwa cyberprzestrzeni w zakresie identyfikacji ryzyk związanych z cyberbezpieczeństwem.
3. W ramach systemu zarządzania ryzykiem w Urzędzie prowadzi się w szczególności następujące rejestry:
   1) rejestr ryzyka do planu działalności – prowadzony przez KOKZ;
   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 pełnomocnika do spraw bezpieczeństwa informacji, którego wzór określa 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.

§ 7. Dyrektorzy zarządzają oraz sprawują nadzór w zakresie zarządzania ryzykiem w kierowanych komórkach organizacyjnych.

§ 8. Do zadań właścicieli ryzyka należy w szczególności:

1) ustalenie kontekstu prowadzonej działalności;
2) weryfikacja poziomu realizacji celów w oparciu o dobór odpowiednich mierników;
3) ocena ryzyk związanych z realizacją celów, za które odpowiadają w zakresie prowadzonej działalności;
4) określenie reakcji w odniesieniu do poszczególnych ryzyk i zaistniałych zagrożeń;
5) wdrażanie działań zaradczych w stosunku do zidentyfikowanych ryzyk;
6) wypełnianie określonych w zarządzeniu obowiązków w zakresie raportowania;
7) bieżąca współpraca z KOKZ i pełnomocnikiem, w tym realizacja otrzymywanych rekomendacji;
8) gromadzenie i analiza informacji o incydentach oraz raportowanie informacji o istotnych incydentach;
9) identyfikowanie i wykorzystywanie szans na efektywną realizację celów i zadań;
10) monitorowanie poziomu ryzyka oraz skuteczności decyzji dotyczących sposobu postępowania z ryzykiem.

§ 9. Dyrektorzy, jako właściciele procesów odpowiedzialni są za realizację czynności przetwarzania, o których mowa w Polityce Bezpieczeństwa Informacji w Urzędzie.

§ 10. Właściciele zasobów 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.

§ 11. 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 niezwłocznie w postaci pisemnej lub elektronicznej KOKZ i pełnomocnika o:

1) zmaterializowaniu się ryzyka;
2) potencjalnych nowych ryzykach lub istotnych zmianach poziomu ryzyk zidentyfikowanych w rejestrach ryzyka;
3) zdarzeniach, które mogą negatywnie wpływać na realizację celów;

4) pojawiających się możliwościach wykorzystania szans.

2. Pracownicy są obowiązani do niezwłocznego informowania przełożonych w postaci pisemnej lub elektronicznej w szczególności 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.
4. Zasady zarządzania i monitorowania ryzyka dotyczącego ciągłości działania Urzędu oraz inwestycji prowadzonych w Urzędzie regulują odrębne przepisy.

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

Rozdział 5

Wyznaczanie celów

§ 13. Zasady wyznaczania celów, ustanawiania mierników realizacji celów, a także zasady monitorowania stopnia realizacji celów określają przepisy odrębne dotyczące zasad funkcjonowania kontroli zarządczej w Urzędzie.

Rozdział 6

Identyfikacja i ocena ryzyka

§ 14. 1. Cyklicznie w terminie do dnia 20 października dyrektorzy dokonują identyfikacji i oceny ryzyka, w odniesieniu do wszystkich celów wskazanych w planie działalności Urzędu na następny rok.
2. W przypadku zmiany celów, o których mowa w ust. 1, właściciele celów przeprowadzają ponowną identyfikację i ocenę ryzyka.
3. W przypadku istotnej zmiany warunków, w których funkcjonuje właściciel ryzyka, dokonuje on ponownej identyfikacji i oceny ryzyka.

§ 15. Ocena ryzyka strategicznego i operacyjnego dokonywana jest również w przypadku istotnej zmiany warunków, w których funkcjonuje Urząd.

§ 16. 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 w szczególności:
   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 albo zmniejszenie, wynikające ze źródeł zewnętrznych i wewnętrznych.
4. Wynik ustaleń, o których mowa w ust. 2 i 3, zawiera się w formie opisu ryzyka.

§ 17. 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.

§ 18. 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;
   4) 4 oznacza, że wdrożone i stosowane mechanizmy kontrolne w znacznym stopniu ograniczają prawdopodobieństwo materializacji ryzyka i siłę jego oddziaływania lub jednego z tych elementów, nie wystąpiły okoliczności, co wpływa na znaczne zmniejszenie oszacowania prawdopodobieństwa wystąpienia ryzyka i siły jego oddziaływania lub jednego z tych elementów o 4 punkty.

§ 19. 1. Matryca ryzyka jest graficzną prezentacją wyników szacowania ryzyka i służy do ustalenia hierarchii ewentualnych działań mających na celu zmniejszenie istotności ryzyka, której wzór określa 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 niezwłocznego opracowania i wdrożenia planu postępowania z ryzykiem bardzo wysokim, który sporządzany jest według wzoru, stanowiącego załącznik nr 4.
3. Przyjmuje się, że ryzyka nieakceptowalne właściciel ryzyka może zaakceptować w przypadku, gdy zastosowano wszystkie możliwe i dostępne mechanizmy kontrolne.
4. Członkowie kierownictwa, właściciel ryzyka ze względu na charakter ryzyka mogą obniżyć poziom ryzyka do akceptowalnego za pomocą odpowiednich mechanizmów kontrolnych.

§ 20. 1. Wyniki oceny ryzyka mają na celu stwierdzenie czy ryzyko, jego istotność i charakter są akceptowalne.

2. Ocena ryzyka wspomaga podejmowanie decyzji o sposobie reakcji na ryzyko.

Rozdział 7
Reakcja na ryzyko

§ 21. 1. Dla każdego zidentyfikowanego, poddanego analizie i ocenie ryzyka, jego właściciel wskazuje jedną z poniższych reakcji:
   1) akceptacja – oznacza tolerowanie, nie podejmowanie żadnych działań zaradczych, rozumienie ewentualnych skutków zdarzenia i świadome godzenie się na nie (w szczególności możliwość przeciwdziałania jest ograniczona lub koszt przeciwdziałania przewyższa potencjalne korzyści);
   2) dzielenie się – częściowe lub całkowite przeniesienie ryzyka na inny podmiot;

3) unikanie – niepodejmowanie lub zaprzestanie działania narażającego na ryzyko (rezygnacja z realizacji celu);
4) 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 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 rezydualnym oraz wniosek o decyzję sporządza i podpisuje kwalifikowanym podpisem elektronicznym właściciel ryzyka niezwłocznie po zidentyfikowaniu ryzyka bardzo wysokiego, a następnie przekazuje w postaci pisemnej lub elektronicznej do KOKZ i udostępnia pełnomocnikowi. .
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 zasięgając opinii pełnomocnika w terminie 30 dni od dnia wpływu do KOKZ i pełnomocnika.

Rozdział 8

Raportowanie o ryzykach

§ 22. W terminie do dnia 20 października każdego roku dyrektorzy przekazują do KOKZ 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:

1) ryzykach związanych z realizacją celów z planu działalności Urzędu na następny rok;
2) wszystkich ryzykach do pozostałych celów i zadań, o których mowa w § 3 w ust. 1 w pkt 2, o istotności większej niż niskie.

§ 23. 1. W ciągu 14 dni kalendarzowych od powzięcia informacji o konieczności jej sporządzenia, dyrektorzy przekazują do KOKZ i innych komórek organizacyjnych zgodnie z właściwością odpowiedzialnych za prowadzenie rejestrów ryzyk, o których mowa w § 6 ust. 3, oraz udostępniają pełnomocnikowi aktualizację rejestru ryzyka, o którym mowa w § 22.

2. Na podstawie nadesłanych informacji KOKZ dokonuje aktualizacji rejestrów ryzyka.
3. W ramach 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 określony w

decyzji Wojewody, o której mowa w przepisach odrębnych dotyczących zasad funkcjonowania kontroli zarządczej w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

§ 24. 1. W terminie do dnia 31 stycznia każdego roku dyrektorzy przekazują KOKZ 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 przypadku zmian organizacyjnych, a w szczególności utworzenia, połączenia lub podziału komórek organizacyjnych, dyrektorzy tych komórek organizacyjnych w terminie 30 dni kalendarzowych od utworzenia, połączenia lub podziału:
   1) sporządzają i przekazują do KOKZ 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;
   2) przekazują do KOKZ i udostępniają pełnomocnikowi informację o ryzykach, których istotność osiągnęła poziom wysoki i bardzo wysoki.

3. W przypadku likwidacji komórki organizacyjnej, w ostatnim dniu jej funkcjonowania dyrektor przekazuje do KOKZ i udostępnia pełnomocnikowi raport ryzyka według stanu na dzień likwidacji.

§ 25. 1. W oparciu o otrzymane informacje KOKZ, w terminie 21 dni roboczych od dnia otrzymania ze wszystkich komórek organizacyjnych poprawnych informacji sporządza:
   1) rejestr ryzyka Urzędu;
   2) aktualizację rejestru ryzyka Urzędu na dany rok;
   3) raport ryzyka Urzędu za zakończony rok.

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

§ 26. 1. Wszystkie informacje i raporty w ramach systemu zarządzania ryzykiem podpisywane są kwalifikowanym podpisem elektronicznym i przekazywane są w systemie EZD, do KOKZ i udostępniane pełnomocnikowi.

2. Rejestr ryzyka, jego aktualizacja, raport ryzyka oraz informacja o zagrożeniach przekazywane do KOKZ i udostępniane pełnomocnikowi w postaci 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 i regulaminach wewnętrznych komórek organizacyjnych Urzędu.

Rozdział 9

Raportowanie o ryzyku w obszarze przetwarzania danych osobowych

§ 27. 1. Dwa razy do roku dyrektorzy mają obowiązek przekazania Inspektorowi Ochrony Danych wypełnioną tabelę zawierającą informacje o występujących w komórkach organizacyjnych ryzykach związanych z przetwarzaniem danych osobowych, które są niezbędne do oszacowania bezpieczeństwa dla danych osobowych przetwarzanych w Urzędzie.

2. Wzór tabeli, o której mowa w ust. 1, określa załącznik nr 3.

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

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

5. Dyrektorzy przekazują wypełnione tabele w terminach:
   1) do dnia 20 października każdego roku na następny rok;
   2) do dnia 31 stycznia każdego roku za rok poprzedni.

6. W oparciu o otrzymane informacje Inspektor Ochrony Danych, w terminie 21 dni roboczych od dnia otrzymania ze wszystkich komórek organizacyjnych poprawnych informacji, sporządza i udostępnia pełnomocnikowi oraz KOKZ informacje w zakresie zidentyfikowanych ryzyk w obszarze przetwarzania danych osobowych oraz ich analizę.

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

8. 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

Raportowanie o ryzyku w obszarze bezpieczeństwa informacji

§ 28. 1. Dwa razy w roku dyrektorzy mają obowiązek przekazania Pełnomocnikowi do spraw Bezpieczeństwa Informacji wypełnioną tabelę zawierającą informacje o występujących w komórkach organizacyjnych ryzykach związanych z bezpieczeństwem informacji, które są niezbędne do oszacowania bezpieczeństwa dla informacji przetwarzanych w Urzędzie.

2. Wzór tabeli, o której mowa w ust. 1, określa załącznik nr 3.

3. Informacje, o których mowa w ust. 1, umożliwią Pełnomocnikowi do spraw Bezpieczeństwa Informacji przygotowanie działań mających na celu poprawę bezpieczeństwa informacji w Urzędzie.

4. Tabele podpisane kwalifikowanym podpisem elektronicznym przez dyrektora należy przesłać w systemie EZD do Pełnomocnika do spraw Bezpieczeństwa Informacji.

5. Dyrektorzy przekazują wypełnione tabele w terminach:
   1) do dnia 20 października każdego roku na następny rok;
   2) do dnia 31 stycznia każdego roku za rok poprzedni.

6. W oparciu o otrzymane informacje, Pełnomocnik do spraw Bezpieczeństwa Informacji, w terminie 21 dni roboczych od dnia otrzymania ze wszystkich komórek organizacyjnych poprawnych informacji, sporządza i udostępnia pełnomocnikowi oraz KOKZ informacje w zakresie zidentyfikowanych ryzyk w obszarze bezpieczeństwa informacji oraz ich analizę.

7. Pełnomocnik do spraw bezpieczeństwa informacji prowadzi rejestr ryzyka Urzędu w obszarze bezpieczeństwa informacji oraz dokonuje aktualizacji rejestru na podstawie uzyskanych informacji o zidentyfikowanych ryzykach.

8. Raport dotyczący identyfikacji i szacowania ryzyka w obszarze bezpieczeństwa informacji Urzędu za zakończony rok wraz z analizą przekazuje się do wiadomości Dyrektorowi Generalnemu Urzędu oraz Zespołowi do spraw Systemu Zarządzania Bezpieczeństwem Informacji.

Rozdział 11

Postanowienia końcowe

§ 29. Rejestr ryzyka, jego aktualizacja, raport ryzyka, w zakresie działalności komórek organizacyjnych rejestruje się w formie elektronicznej wspierającej proces zarządzania ryzykiem w Urzędzie.

§ 30. 1. Działania podejmowane w ramach systemu zarządzania ryzykiem uwzględnia się 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.

§ 31. Nadzór nad wykonaniem zarządzenia powierza się w zakresie posiadanych uprawnień, Dyrektorowi Generalnemu Urzędu oraz Dyrektorowi Biura Kadr, Płac i Budżetu w Urzędzie.

§ 32. Traci moc zarządzenie nr 395 Wojewody Mazowieckiego z dnia 30 października 2020 r. w sprawie polityki zarządzania ryzykiem w Mazowieckim Urzędzie Wojewódzkim w Warszawie.

§ 33. Zarządzenie wchodzi w życie z dniem podpisania, z mocą od dnia 31 marca 2025 r.

WOJEWODA MAZOWIECKI
Mariusz Frankowski
/podpisano kwalifikowanym
podpisem elektronicznym/