Załącznik do uchwały nr 58/287/22
Zarządu Województwa Mazowieckiego
z dnia 18 stycznia 2022 r.

REGULAMIN AUDYTU BEZPIECZEŃSTWA INFORMACJI

Rozdział 1

Przepisy ogólne

§ 1.

1. Regulamin audytu bezpieczeństwa informacji określa:
   1) zasady przeprowadzania audytów w zakresie ochrony danych osobowych przetwarzanych w Urzędzie oraz u dostawców Urzędu, z którymi zawarto umowy powierzenia przetwarzania danych osobowych, oraz w zakresie zgodności z wymogami normy PN-EN ISO/IEC 27001:2017-06;
   2) obowiązki i uprawnienia audytora oraz pracowników audytowanych komórek organizacyjnych Urzędu lub dostawców.
2. Użyte w regulaminie określenia oznaczają:
   1) ADO – administratora danych osobowych, o którym mowa w art. 4 pkt 7 RODO; w rozumieniu niniejszego regulaminu ADO jest, stosownie do danej czynności przetwarzania, Województwo Mazowieckie, Zarząd Województwa Mazowieckiego, Marszałek Województwa Mazowieckiego lub Urząd Marszałkowski Województwa Mazowieckiego;
   2) audyt – audyt bezpieczeństwa informacji polegający na weryfikacji zgodności przetwarzania danych z przepisami prawa, umowami oraz regulacjami wewnątrzorganizacyjnymi, a także zgodności z wymogami normy;
   3) audytor – kierownika lub pracownika Biura Bezpieczeństwa Informacji w Departamencie Organizacji Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie lub osobę przeprowadzającą audyt na podstawie upoważnienia udzielonego przez ADO albo przez osobę upoważnioną do kontroli umów powierzenia przetwarzania danych osobowych;
   4) departament/kancelaria – komórkę organizacyjną Urzędu, w której przeprowadza się audyt;
   5) dostawca – podmiot zewnętrzny, z którym zawarto umowę w zakresie świadczenia usług na rzecz Urzędu, w tym podmioty przetwarzające w rozumieniu art. 4 pkt 8 RODO;
   6) IOD – Inspektora ochrony danych, wyznaczonego przez ADO, zgodnie z art. 37 RODO;
   7) Kierownik BBI – kierownika Biura Bezpieczeństwa Informacji w Departamencie Organizacji Urzędu;
   8) niezgodność – niezgodność z wymogami normy, przepisami prawa, umowami lub regulacjami wewnątrzorganizacyjnymi w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych;
   9) norma – normę Międzynarodowej Organizacji Normalizacyjnej PN-EN ISO/IEC 27001:2017-06;
   10) podmiot przetwarzający – podmiot, o którym mowa w art. 4 pkt 8 RODO, któremu ADO powierzył przetwarzanie danych osobowych;
   11) RODO – rozporządzenie Parlamentu Europejskiego Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
   12) upoważnienie – upoważnienie do przeprowadzenia audytu udzielone przez ADO lub przez osobę umocowaną do działania w imieniu ADO;
   13) Urząd – Urząd Marszałkowski Województwa Mazowieckiego w Warszawie.

§ 2.

1. Audyty mogą być przeprowadzane jako audyty planowe lub audyty doraźne.
2. Podstawą przeprowadzania audytu planowego jest zaakceptowany przez Sekretarza Województwa – Dyrektora Urzędu oraz właściwego ADO plan audytów.
3. Podstawą przeprowadzania audytu doraźnego jest zlecenie przeprowadzenia audytu doraźnego.

§ 3.

1. Audyty planowe prowadzi się na podstawie rocznych planów audytów.
2. Roczny plan audytów opracowuje kierownik BBI przy współudziale Pełnomocnika ds. zintegrowanego systemu zarządzania do 20 grudnia roku poprzedniego.
3. Po zatwierdzeniu przez Sekretarza Województwa – Dyrektora Urzędu, roczny plan audytów wymaga akceptacji właściwego ADO.
4. Roczny plan audytów w szczególności zawiera:
   1) nazwę audytowanego departamentu/kancelarii lub dostawcy;
   2) zakres audytu;
   3) kryteria audytu;
   4) termin przeprowadzenia audytu.
5. Roczny plan audytów jest publikowany na stronie intranetowej Urzędu.
6. Do zmian Rocznego planu audytów ust. 3 stosuje się odpowiednio.

§ 4.

1. W przypadkach stwierdzenia okoliczności wymagających podjęcia natychmiastowych działań z uwagi na zagrożenie bezpieczeństwa informacji, kierownik BBI podejmuje działania opisane w odpowiednim procesie w Księdze Zarządzania Procesami Zintegrowanego Systemu Zarządzania, dotyczącym zarządzania incydentami związanymi z bezpieczeństwem informacji.
2. Postępowanie z niezgodnościami prowadzone jest zgodnie z procesem dotyczącym nadzoru nad wyrobem niezgodnym, opisanym w Księdze Zarządzania Procesami Zintegrowanego Systemu Zarządzania.

§ 5.

1. Audyty doraźne mają charakter interwencyjny, w szczególności wynikający z potrzeby zbadania nagłych zdarzeń, na postawie informacji otrzymanych przez IOD, kierownika BBI lub Pełnomocnika ds. zintegrowanego systemu zarządzania, w szczególności w celu:
   1) zbadania określonych spraw związanych z bezpieczeństwem informacji, w tym ochroną danych osobowych, wynikających ze skarg lub sygnałów wpływających do Urzędu;
   2) pilnego zbadania nagłych i nieprzewidzianych zdarzeń związanych z bezpieczeństwem informacji.
2. Audyty doraźne prowadzi się na podstawie zlecenia wydanego przez Sekretarza Województwa – Dyrektora Urzędu.
3. Dyrektor departamentu/kancelarii oraz IOD mogą wystąpić do Sekretarza Województwa – Dyrektora Urzędu z wnioskiem o przeprowadzenie audytu doraźnego, wraz z uzasadnieniem.
4. W przypadku przeprowadzenia audytu doraźnego nie mają zastosowania zasady wynikające z § 7, § 8 ust. 1 oraz § 11.
5. Do przeprowadzenia audytu doraźnego stosuje się odpowiednio postanowienia: § 8 ust. 2-5, § 9, § 10, § 12-14.

§ 6.

Kierownik BBI przedkłada Sekretarzowi Województwa – Dyrektorowi Urzędu, właściwemu ADO, Pełnomocnikowi ds. zintegrowanego systemu, Pełnomocnikowi ds. cyberbezpieczeństwa oraz IOD roczne sprawozdanie z wykonania planu audytów oraz z audytów doraźnych.

Rozdział 2

Audyt prowadzony w Urzędzie

Oddział 1

Postanowienia ogólne

§ 7.

Audyt planowy w Urzędzie prowadzony jest przez co najmniej dwóch audytorów.

§ 8.

1. O planowanym audycie audytor powiadamia dyrektora departamentu/kancelarii z 7-dniowym wyprzedzeniem.
2. Audyt przeprowadza się w godzinach pracy Urzędu.
3. Audytorzy przed przystąpieniem do czynności audytowych mają obowiązek okazania legitymacji służbowej, chyba że audyt prowadzony jest w formie zdalnej.
4. Audytorom w czasie wykonywania czynności audytowych może towarzyszyć inny pracownik Urzędu – w charakterze eksperta.
5. Pracownik, o którym mowa w ust. 4, w terminie wskazanym przez audytora, sporządza pisemną notatkę z przeprowadzonych czynności, którą następnie dołącza się do dokumentów audytu.

Oddział 2

Uprawnienia audytorów i audytowanych

§ 9.

1. W ramach czynności audytowych audytorzy mają prawo:
   1) wglądu do dokumentów objętych zakresem audytu, w celu weryfikacji ich zawartości oraz jeżeli zajdzie taka konieczność, do sporządzenia kopii;
   2) dostępu do wszystkich pomieszczeń departamentu/kancelarii, w celu przeprowadzenia oględzin dokumentowanych notatką z oględzin lub zdjęciami;
   3) dostępu do wszystkich systemów informatycznych departamentu/kancelarii oraz wszelkich nośników informacji, których weryfikacja jest niezbędna do przeprowadzenia audytu, w celu weryfikacji ich zawartości oraz sposobów ich zabezpieczenia;
   4) wykonywania zdjęć pomieszczeniom, dokumentom oraz innym nośnikom informacji;
   5) żądania od dyrektora lub pracownika departamentu/kancelarii ustnych lub pisemnych wyjaśnień.
2. Dyrektor departamentu/kancelarii zapewnia audytorom warunki i środki techniczne niezbędne do sprawnego przeprowadzenia audytu.
3. Pracownicy departamentu/kancelarii mają obowiązek współpracować z audytorami celem sprawnego przeprowadzenia audytu.
4. Dyrektor departamentu/kancelarii lub wyznaczony przez niego pracownik mają prawo do czynnego uczestniczenia w każdym etapie audytu.
5. W przypadku, gdy działania/zaniechania departamentu/kancelarii utrudniają realizację czynności audytowych, audytor informuje o zaistniałym stanie Sekretarza Województwa – Dyrektora Urzędu, oraz zawiesza prowadzenie audytu do czasu decyzji Sekretarza Województwa – Dyrektora Urzędu.
6. Za działania/zaniechania, o których mowa w ust. 5, rozumie się w szczególności nieprzedstawienie do audytu dokumentów lub materiałów niezbędnych do przeprowadzenia audytu, składanie wyjaśnień uniemożliwiających jednoznaczne określenie stanu faktycznego oraz zachowanie utrudniające realizację przez audytorów czynności, o których mowa w ust. 1.

Oddział 3

Dokumentacja czynności audytowych

§ 10.

1. Audytorzy sporządzają protokół z audytu planowego w terminie 30 dni od dnia zakończenia audytu, przez co rozumie się dzień realizacji ostatniej czynności realizowanej przy udziale audytowanego departamentu/kancelarii. Protokół sporządza się wyłącznie w formie elektronicznej.
2. Protokół, o którym mowa w ust. 1, powinien zawierać:
   1) nazwę departamentu/kancelarii oraz imię i nazwisko dyrektora departamentu/kancelarii;
   2) imiona i nazwiska audytorów oraz osób biorących udział w audycie;
   3) termin przeprowadzenia audytu – datę rozpoczęcia i zakończenia audytu;
   4) zakres przedmiotowy audytu;
   5) opis stanu faktycznego stwierdzonego w toku czynności audytowych;
   6) ewentualnie stwierdzone niezgodności;
   7) ewentualne rekomendacje.
3. Kierownik BBI podpisuje protokół z przeprowadzonego audytu, a następnie, po ewentualnej akceptacji Sekretarza Województwa-Dyrektora Urzędu, przekazuje protokół dyrektorowi departamentu/kancelarii oraz do wiadomości IOD.
4. Dyrektor departamentu/kancelarii, w terminie 7 dni od dnia otrzymania protokołu, odsyła do kierownika BBI podpisany elektronicznie protokół. W przypadku stwierdzenia niezgodności, dyrektor departamentu/kancelarii załącza do protokołu dodatkowe wyjaśnienia dla Sekretarza Województwa-Dyrektora Urzędu.
5. Do podpisanego protokołu mogą być załączone zastrzeżenia o charakterze formalnym, dotyczące ustalonego stanu faktycznego.
6. Kierownik BBI opracowuje stanowisko do zgłoszonych wyjaśnień lub zastrzeżeń i przekazuje całość dokumentacji do Sekretarza Województwa – Dyrektora Urzędu celem ewentualnego podjęcia decyzji o sposobie dalszego postępowania.
7. Dokumentacja związana z audytem prowadzona jest w formie elektronicznej przez Biuro Bezpieczeństwa Informacji w Departamencie Organizacji Urzędu.

Rozdział 3

Audyt dostawców

Oddział 1

Postanowienia ogólne

§ 11.

Audyt planowy prowadzony jest przez co najmniej dwóch audytorów.

§ 12.

1. Audytor powiadamia dostawcę o planowanym audycie w terminie określonym w umowie zawartej z dostawcą lub innym instrumencie prawnym, będącym podstawą prowadzonego audytu, a jeśli termin nie został określony, co najmniej 7 dni przed rozpoczęciem audytu.
2. Audyt przeprowadza się w godzinach pracy dostawcy.
3. Audytorzy przed przystąpieniem do czynności audytowych mają obowiązek okazania legitymacji służbowej oraz upoważnienia, którego wzór stanowi załącznik do niniejszego regulaminu, a jeżeli audyt prowadzony jest w formie zdalnej – audytorzy przesyłają skany upoważnień.

Oddział 2

Uprawnienia audytorów i audytowanych

§ 13.

1. W ramach czynności audytowych audytorzy mają prawo:
   1) wglądu do dokumentów regulujących zasady bezpieczeństwa informacji w podmiocie przetwarzającym, w szczególności: Polityki bezpieczeństwa, rejestru wszystkich kategorii czynności, rejestru umów powierzenia przetwarzania danych, rejestru naruszeń, rejestru upoważnień oraz upoważnień do przetwarzania danych osobowych, stosowanych klauzul informacyjnych, przyjętych zgód na przetwarzanie danych osobowych – wyłącznie w zakresie odnoszącym się do świadczonej przez dostawcę usługi;
   2) wglądu do dokumentów zawierających powierzone informacje, w tym w szczególności dane osobowe w celu weryfikacji ich zawartości oraz jeżeli zajdzie taka konieczność, do sporządzenia ich kopii;
   3) dostępu do pomieszczeń, w których przetwarzane są informacje związane z realizacją usługi, w celu przeprowadzenia oględzin dokumentowanych notatką z oględzin;
   4) dostępu do systemów informatycznych dostawcy, w których przetwarzane są dane osobowe powierzone przez właściwego ADO oraz wszelkich innych informacji, których weryfikacja jest niezbędna do przeprowadzenia audytu, w celu weryfikacji ich zawartości oraz sposobów ich zabezpieczenia, o ile służą do realizacji świadczonej usługi;
   5) wykonywania zdjęć pomieszczeniom, dokumentom oraz innym nośnikom informacji, w celu udokumentowania czynności, o których mowa w pkt 1-4;
   6) żądania od osób reprezentujących podmiot przetwarzający lub pracownika dostawcy ustnych lub pisemnych wyjaśnień.
2. Osoby reprezentujące dostawcę zapewniają audytorom warunki i środki techniczne niezbędne do sprawnego przeprowadzenia audytu.
3. Audytorzy są zobowiązani do zachowania poufności wszelkich informacji jakie uzyskają w trakcie prowadzonego audytu.
4. Uprawnienia określone w ust. 1 mogą być ograniczane ze względu na tajemnicę przedsiębiorstwa, jednak nie może to uniemożliwiać realizacji audytu. W przypadku wystąpienia takiego ograniczenia, audytorzy przyjmują w ww. zakresie pisemne wyjaśnienia od dostawcy.
5. Osoby reprezentujące dostawcę, u którego przeprowadzany jest audyt, lub wyznaczony przez niego pracownik mają prawo do czynnego uczestniczenia w każdym etapie audytu.
6. W przypadku, gdy działania/zaniechania dostawcy utrudniają realizację czynności audytowych, audytor informuje o zaistniałym stanie właściwego Sekretarza Województwa – Dyrektora Urzędu i zawiesza prowadzenie audytu do czasu podjęcia decyzji przez Sekretarza Województwa – Dyrektora Urzędu o dalszym sposobie postępowania.
7. Za działania/zaniechania, o których mowa w ust. 6, rozumie się w szczególności nieprzedstawienie do audytu dokumentów lub materiałów niezbędnych do przeprowadzenia audytu, składanie wyjaśnień uniemożliwiających jednoznaczne określenie stanu faktycznego oraz zachowanie utrudniające realizację przez audytorów czynności, o których mowa w ust. 1.

Oddział 3

Dokumentacja czynności audytowych

§ 14.

1. Audytorzy sporządzają protokół z audytu planowego w terminie 30 dni od dnia zakończenia audytu, przez co rozumie się dzień realizacji ostatniej czynności realizowanej przy udziale dostawcy. Protokół sporządza się w formie elektronicznej, chyba że umowa zawarta z dostawcą nie dopuszcza możliwości elektronicznego dostarczenia dokumentu.
2. Protokół, o którym mowa w ust. 1, powinien w szczególności zawierać:
   1) nazwę dostawcy oraz imię i nazwisko osoby reprezentującej;
   2) imiona i nazwiska audytorów oraz osób biorących udział w audycie;
   3) zwięzły opis działań dostawcy w obszarze objętym audytem;
   4) termin przeprowadzenia audytu – datę rozpoczęcia i zakończenia audytu;
   5) zakres przedmiotowy audytu;
   6) opis stanu faktycznego stwierdzonego w toku przeprowadzanego audytu;
   7) ewentualnie stwierdzone niezgodności;
   8) ewentualne rekomendacje.
3. Kierownik BBI podpisuje protokół z przeprowadzonego audytu, a następnie, przekazuje protokół do ewentualnej akceptacji Sekretarza Województwa – Dyrektora Urzędu oraz do wiadomości IOD.
4. Po akceptacji protokołu przez Sekretarza Województwa – Dyrektora Urzędu, protokół z przeprowadzonego audytu przekazuje się dostawcy.
5. W terminie 7 dni od otrzymania protokołu dostawca może zgłosić uzasadnione zastrzeżenia do protokołu.
6. W przypadku zgłoszenia zastrzeżeń, o których mowa w ust. 6, kierownik BBI w terminie 7 dni przygotowuje stanowisko do zastrzeżeń, które z wykorzystaniem drogi służbowej przekazuje do osoby akceptującej protokół w celu ewentualnego podjęcia decyzji o dalszym sposobie postępowania.
7. Dokumentacja związana z audytem prowadzona jest w formie elektronicznej przez Biuro Bezpieczeństwa Informacji w Departamencie Organizacji Urzędu.

Załącznik do *Regulaminu audytu bezpieczeństwa informacji*

Wzór upoważnienie do przeprowadzenia audytu

Warszawa, [data]

UPOWAŻNIENIE

Na podstawie [*uchwały Zarządu Województwa Mazowieckiego nr ….. z dnia ……r.*] w związku z art. 28 ust. 3 lit. h rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 04.05.2016 r., str. 1, z późn. zm.; dalej zwanego „RODO")

upoważniam

Panią/Pana [*imię i nazwisko*]

zatrudnionego [*stanowisko/funkcja*]

do przeprowadzenia audytu w [*nazwa dostawcy*],

w zakresie spełnienia obowiązków określonych w art. 28 RODO oraz w umowie [*nr i data umowy*].

Audyt zostanie rozpoczęty w dniu [*data*].

W ramach audytu, osoba upoważniona uprawniona jest do podejmowania wszystkich czynności określonych w *Regulaminie audytu bezpieczeństwa informacji* – w granicach wynikających z zapisów ww. Regulaminu oraz umowy, której spełnienie obowiązków dotyczy audyt.

…….. ……..

Administrator danych osobowych