Załącznik do uchwały nr 1676/179/20
Zarządu Województwa Mazowieckiego
z dnia 3 listopada 2020 r.

REGULAMIN AUDYTU OCHRONY DANYCH OSOBOWYCH, KTÓRYCH ADMINISTRATOREM JEST WOJEWÓDZTWO MAZOWIECKIE LUB ZARZĄD WOJEWÓDZTWA MAZOWIECKIEGO

Dział I

Przepisy ogólne

§ 1.

1. Regulamin audytu ochrony danych osobowych, których administratorem jest Województwo Mazowieckie lub Zarząd Województwa Mazowieckiego określa zasady przeprowadzania audytów w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie oraz podmiotach przetwarzających, obowiązki i uprawnienia audytora oraz pracowników audytowanych komórek organizacyjnych Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie lub podmiotu przetwarzającego.
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 albo Zarząd Województwa Mazowieckiego;
   2) audyt – audyt ochrony danych osobowych polegający na weryfikacji zgodności przetwarzania danych osobowych z zasadami przetwarzania danych osobowych;
   3) audytor – IOD, pracownika Biura Bezpieczeństwa Informacji w Departamencie Organizacji Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie lub osobę przeprowadzająca audyt na podstawie upoważnienia udzielonego przez ADO albo przez osobę upoważnioną do kontroli umów powierzenia przetwarzania danych osobowych;
   4) IOD – Inspektora ochrony danych, wyznaczonego przez ADO, zgodnie z art. 37 RODO;
   5) departament/kancelaria – komórkę organizacyjną Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie, w której przeprowadza się audyt;
   6) dyrektor departamentu/kancelarii – osobę kierującą odpowiednio departamentem lub kancelarią w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie;
   7) nieprawidłowość – niezgodność z przepisami prawa, umowami lub regulacjami wewnętrznymi mogąca powodować lub powodująca naruszenie ochrony danych osobowych mogące powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych lub w znacznym stopniu osłabiające system ochrony danych osobowych;
   8) podmiot przetwarzający – podmiot, o którym mowa w art. 4 pkt 8 RODO, któremu ADO powierzył przetwarzanie danych osobowych;
   9) 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);
   10) uchybienie – niezgodności z przepisami prawa, umowami lub regulacjami wewnętrznymi mające charakter formalny lub niewielkiej wagi;
   11) upoważnienie – upoważnienie do przeprowadzenia audytu w podmiocie przetwarzającym, udzielone przez ADO lub w imieniu ADO przez osobę, która zawarła w imieniu ADO daną umowę powierzenia przetwarzania danych osobowych;
   12) 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 właściwego ADO plan audytów.

3. Podstawą przeprowadzania audytu doraźnego jest zlecenie przeprowadzenia audytu doraźnego.

§ 3.

1. Audyty planowe prowadzi się na podstawie półrocznych planów audytów.
2. Półroczny plan audytów opracowuje IOD w terminie:
   1) na pierwsze półrocze danego roku – do 20 grudnia roku poprzedniego;
   2) na drugie półrocze danego roku – do 20 czerwca danego roku.
3. Po zatwierdzeniu przez Sekretarza Województwa – Dyrektora Urzędu, półroczny plan audytów wymaga akceptacji właściwego ADO.
4. Półroczny plan audytów powinien w szczególności zawierać:
   1) nazwę audytowanego departamentu/kancelarii lub podmiotu przetwarzającego;
   2) zakres audytu;
   3) termin przeprowadzenia audytu.
5. Półroczny plan audytów jest publikowany na stronie intranetowej Urzędu.
6. Do zmian półrocznego planu audytów ma zastosowanie odpowiednio ust. 3.

§ 4.

1. Audyty doraźne mają charakter interwencyjny, w szczególności wynikający z potrzeby zbadania nagłych zdarzeń, na postawie informacji otrzymanych przez IOD, w szczególności w celu:
   1) zbadania określonych spraw związanych z ochroną danych osobowych wynikających ze skarg lub sygnałów wpływających do Urzędu;
   2) pilnego zbadania nagłych i nieprzewidzianych zdarzeń związanych z ochroną danych osobowych.
2. Audyty doraźne prowadzi się na podstawie zlecenia wydanego przez właściwego ADO lub Sekretarza Województwa – Dyrektora Urzędu, a w przypadku audytów prowadzonych w Urzędzie, również na podstawie decyzji IOD.
3. Dyrektor departamentu/kancelarii Urzędu może wystąpić do właściwego ADO, Sekretarza Województwa – Dyrektora Urzędu lub IOD z wnioskiem o przeprowadzenie audytu doraźnego, wraz z uzasadnieniem. W przypadku wniosku skierowanego do IOD, IOD informuje Sekretarza Województwa – Dyrektora Urzędu o planowanym przeprowadzeniu w Urzędzie audytu na podstawie wniosku albo przekazuje wniosek do Sekretarza Województwa – Dyrektora Urzędu wraz ze wstępną oceną jego zasadności.
4. W przypadku przeprowadzenia audytu doraźnego nie mają zastosowania zasady wynikające z § 7 ust. 1, § 10 i § 13 ust. 1.
5. Audyt doraźny w podmiocie przetwarzającym może być przeprowadzony przez jednego audytora.
6. Protokół z audytu doraźnego należy przygotować w terminie 14 dni od dnia zakończenia audytu, przez co rozumie się dzień realizacji ostatniej czynności realizowanej przy udziale audytowanego departamentu/kancelarii lub podmiotu przetwarzającego. Protokół sporządza się w 2 egzemplarzach.
7. Do przeprowadzenia audytu doraźnego stosuje się odpowiednio postanowienia: § 6, § 7 ust. 2-5, § 8, § 9, § 11–12 i § 13 ust. 2-7.

§ 5.

1. IOD opracowuje półroczne sprawozdania z wykonania planu audytów oraz z audytów doraźnych.
2. Sprawozdania, o których mowa w ust. 1, po ich zatwierdzeniu przez Sekretarza Województwa – Dyrektora Urzędu, przedkładane są do właściwego ADO.

Dział II

Audyt prowadzony w Urzędzie

Rozdział I

Postanowienia ogólne

§ 6.

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

§ 7.

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.

Rozdział II

Uprawnienia audytorów

§ 8.

1. W ramach czynności audytowych audytorzy mają prawo:
   1) wglądu do wszystkich dokumentów w departamencie/kancelarii, 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, w szczególności polegające na nieprzedstawieniu do audytu dokumentów lub materiałów niezbędnych do przeprowadzenia audytu, składaniu wyjaśnień uniemożliwiających jednoznaczne określenie stanu faktycznego, audytor ma obowiązek poinformować o zaistniałym stanie właściwego ADO lub Sekretarza Województwa – Dyrektora Urzędu, oraz zawiesza prowadzenie audytu do czasu decyzji ADO lub Sekretarza Województwa – Dyrektora Urzędu.
6. W przypadkach stwierdzenia okoliczności wymagających podjęcia natychmiastowych działań z uwagi na zagrożenie bezpieczeństwa danych osobowych, IOD może równolegle podjąć działania opisane w odpowiednim procesie w Księdze Zarządzania Procesami Zintegrowanego Systemu Zarządzania, dotyczące postępowania w sytuacji naruszenia ochrony danych osobowych.

Rozdział III

Dokumentacja czynności audytowych

§ 9.

1. Audytorzy sporządzają protokół z audytu planowego w terminie 14 dni od dnia zakończenia audytu, przez co rozumie się dzień realizacji ostatniej czynności realizowanej przy udziale audytowanego departamentu/kancelarii. Protokół sporządza się w dwóch egzemplarzach.
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 uchybienia lub nieprawidłowości;
   7) ewentualne rekomendacje.
3. IOD zatwierdza protokół z przeprowadzonego audytu, a następnie z wykorzystaniem drogi służbowej przekazuje jeden egzemplarz do dyrektora departamentu/kancelarii.
4. Dyrektor departamentu/kancelarii, w terminie 7 dni od dnia otrzymania protokołu, odsyła do IOD podpisany egzemplarz protokołu. Jeden egzemplarz protokołu zostaje u dyrektora departamentu/kancelarii. W przypadku stwierdzenia nieprawidłowości, dyrektor departamentu/kancelarii załącza do protokołu dodatkowe wyjaśnienia dla ADO.
5. Do podpisanego protokołu mogą być załączone zastrzeżenia o charakterze formalnym, dotyczące ustalonego stanu faktycznego.
6. IOD z wykorzystaniem drogi służbowej przekazuje protokół oraz ewentualne zastrzeżenia do protokołu wraz ze stanowiskiem IOD do zastrzeżeń do Sekretarza Województwa – Dyrektora Urzędu, w celu ewentualnego podjęcia decyzji o sposobie dalszego postępowania.
7. Jeżeli podczas audytu zostaną stwierdzone nieprawidłowości, IOD dodatkowo przekazuje dokumenty, o których mowa w ust. 6, wraz z informacją o podjętych lub planowanych działaniach do właściwego ADO.
8. Dokumentacja związana z przeprowadzonym audytem przechowywana jest w Biurze Bezpieczeństwa Informacji w Departamencie Organizacji Urzędu.

Dział III

Audyt prowadzony w podmiocie przetwarzającym

Rozdział I

Postanowienia ogólne

§ 10.

Audyt planowy prowadzony jest przez zespół w skład którego wchodzi co najmniej IOD oraz drugi audytor.

§ 11.

1. Audytor powiadamia podmiot przetwarzający o planowanym audycie w terminie określonym w umowie powierzenia przetwarzania danych osobowych zawartej pomiędzy właściwym ADO i podmiotem przetwarzającym.
2. Audyt przeprowadza się w godzinach pracy podmiotu przetwarzającego.
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.

Rozdział II

Uprawnienia audytorów

§ 12.

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 przetwarzania danych osobowych powierzonego przez ADO;
   2) wglądu do dokumentów zawierających powierzone przez właściwego ADO dane osobowe, w celu weryfikacji ich zawartości oraz jeżeli zajdzie taka konieczność, do sporządzenia ich kopii;
   3) dostępu do pomieszczeń, w których przetwarzane są dane osobowe powierzone przez właściwego ADO, w celu przeprowadzenia oględzin dokumentowanych notatką z oględzin;
   4) dostępu do systemów informatycznych podmiotu przetwarzającego, w których przetwarzane są dane osobowe powierzone przez właściwego ADO oraz wszelkich innych źródeł informacji, których weryfikacja jest niezbędna do przeprowadzenia audytu, w celu weryfikacji ich zawartości oraz sposobów ich zabezpieczenia, o ile służą do realizacji przetwarzania danych osobowych powierzonego przez ADO;
   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 podmiotu przetwarzającego ustnych lub pisemnych wyjaśnień.
2. Osoby reprezentujące podmiot przetwarzający 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 podmiotu przetwarzającego.
5. Wszyscy pracownicy podmiotu przetwarzającego mają obowiązek współpracować z audytorami celem sprawnego przeprowadzenia audytu.
6. Osoby reprezentujące podmiot przetwarzający, w którym przeprowadzany jest audyt, lub wyznaczony przez nich pracownik mają prawo do czynnego uczestniczenia w każdym etapie audytu.
7. W przypadku, gdy działania/zaniechania podmiotu przetwarzającego utrudniają realizację czynności audytowych, w szczególności polegające na nieprzedstawieniu do audytu dokumentów lub materiałów niezbędnych do przeprowadzenia audytu, składaniu wyjaśnień uniemożliwiających jednoznaczne określenie stanu faktycznego, audytor ma obowiązek poinformować o zaistniałym stanie rzeczy Sekretarza Województwa – Dyrektora Urzędu, oraz zawiesza prowadzenie audytu do czasu podjęcia decyzji przez Sekretarza Województwa – Dyrektora Urzędu o dalszym sposobie postępowania.
8. W przypadkach stwierdzenia okoliczności wymagających podjęcia natychmiastowych działań z uwagi na zagrożenie bezpieczeństwa danych osobowych, audytor może równolegle podjąć działania opisane w odpowiednim procesie w Księdze Zarządzania Procesami Zintegrowanego Systemu Zarządzania, dotyczące postępowania w sytuacji naruszenia ochrony danych osobowych.

Rozdział III

Dokumentacja czynności audytowych

§ 13.

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 podmiotu przetwarzającego. Protokół sporządza się w dwóch egzemplarzach.
2. Protokół, o którym mowa w ust. 1, powinien w szczególności zawierać:
   1) nazwę podmiotu przetwarzającego oraz imię i nazwisko osoby reprezentującej;
   2) imiona i nazwiska audytorów oraz osób biorących udział w audycie;
   3) zwięzły opis działań podmiotu przetwarzającego 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 uchybienia lub nieprawidłowości;
   8) ewentualne rekomendacje.
3. IOD zatwierdza protokół z przeprowadzonego audytu, a następnie z wykorzystaniem drogi służbowej przekazuje do Sekretarza Województwa – Dyrektora Urzędu, w celu ewentualnego podjęcia decyzji o sposobie dalszego postępowania.
4. Jeżeli podczas audytu zostaną stwierdzone nieprawidłowości, IOD przekazuje protokół z przeprowadzonego audytu wraz z informacją o podjętych lub planowanych działaniach do właściwego ADO.
5. Po akceptacji protokołu przez Sekretarza Województwa – Dyrektora Urzędu, a w przypadku stwierdzenia nieprawidłowości – przez właściwego ADO, jeden egzemplarz protokołu z przeprowadzonego audytu przekazuje się podmiotowi przetwarzającemu, który w terminie 7 dni od dnia otrzymania protokołu może zgłosić uzasadnione zastrzeżenia.
6. W przypadku zgłoszenia zastrzeżeń, o których mowa w ust. 5, IOD 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 związaną z przeprowadzonym audytem przechowywana jest w Biurze Bezpieczeństwa Informacji w Departamencie Organizacji Urzędu.

Załącznik do *Regulaminu audytu ochrony danych osobowych, których administratorem jest Województwo Mazowieckie lub Zarząd Województwa Mazowieckiego*

Wzór upoważnienie do przeprowadzenia audytu

Warszawa, [data]

UPOWAŻNIENIE

Na podstawie [*uchwały Zarządu Województwa Mazowieckiego nr ….. z dnia ……r.*] w związku z art. 28 ust. 1 i 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 podmiotu przetwarzającego*],

w zakresie spełnienia obowiązków określonych w art. 28 RODO oraz w umowie powierzenia przetwarzania danych osobowych [*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 ochrony danych osobowych, których administratorem jest Województwo Mazowieckie lub Zarząd Województwa Mazowieckiego* – w granicach wynikających z zapisów ww. Regulaminu oraz umowy, której spełnienie obowiązków dotyczy audyt.

…….. ……..

Administrator danych osobowych