AUDYTY KRI

Usługa adresowana do instytucji publicznych

KRÓTKA INFORMACJA O AUDYCIE

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności nakłada na rejestry publiczne i wymiany informacji w postaci elektronicznej oraz systemy teleinformatyczne minimalne wymagania jakie powyższe systemu muszą spełnić. W rozporządzeniu nałożony został również obowiązek okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji. **Audyt musi odbywać się nie rzadziej niż raz na rok.**

(..."każdy podmiot publiczny zobowiązany jest do zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok (§ 20 ust.2 pkt 14). " ...)

Omawiane Rozporządzenie to akt wykonawczy do Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne

KOGO DOTYCZY ROZPORZĄDZENIE KRI ?

Rozporządzenie dotyczy podmiotów publicznych, w których przetwarzane są rejestry publiczne w postaci teleinformatycznej. Powinni się dostosować do niego:

- Urzędy Miast i Gmin;
- Starostwa Powiatowe;
- jednostki organizacyjne, np. szkoły, przedszkola, MOPS/GOPS, PCPR, biblioteki, ośrodki kultury;
- podmioty publiczne, np. sądy, stowarzyszenia, kluby sportowe, organizacje rządowe.

KORZYŚCI DLA PODMIOTU

- Pewność zgodności posiadanych systemów i bezpieczeństwa z wymaganiami prawnymi
- Spełnienie wymogów ustawowych
- Eliminacja negatywnych uwag przeprowadzanych przez jednostki nadrzędne
- Znajomość mocnych i słabych stron posiadanej infrastruktury oraz systemów informatycznych
- Minimalizacja ryzyka

CO OBEJMUJE PRZEPROWADZANY PRZEZ NAS AUDYT ?

audyt jest przeprowadzany w obszarach (zakres podstawowy wymagany Rozporządzeniem):

- Polityki bezpieczeństwa i aspektów prawnych,
- Organizacji bezpieczeństwa informacji,
- Zarządzania aktywami,
- Bezpieczeństwa fizycznego, kontroli dostępu i zarządzenia incydentami,
- Zarządzania systemami i sieciami.
- Utrzymania systemów informatycznych,
- Ciągłości działania,
- Analizy ryzyka,
- Zgodności z KRI i RODO
- Przygotowania i przedstawienia sprawozdania z audytu,
- Przekazania propozycji ewentualnych działań naprawczych

JAKIE SĄ KOSZTY PRZEPROWADZENIA AUDYTU W PODMIOCIE PUBLICZNYM ?

Koszt przeprowadzenia audytu jest określony indywidualnie w zależności od warunków zapewnienia bezpieczeństwa informacji i wielkości podmiotu. Nasz audyt w zakresie podstawowym jest przeprowadzony zdalnie. Dzięki temu oraz współpracy z podmiotem przy zbieraniu danych audytowych, koszty zostały znacząco zmniejszone, a wymóg wskazany w Rozporządzeniu - spełniony.

JAKIE SĄ WYTYCZNE DOTYCZĄCE PRZEPROWADZENIA AUDYTU ?

Aby ułatwić podmiotom publicznym realizację nałożonych na nie zadań, Departament Informatyzacji MAC i Departament Audytu Sektora Finansów Publicznych MF przygotowały wspólne stanowisko dotyczące zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji. W dokumencie stwierdzono, że intencją autorów rozporządzenia w sprawie systemów teleinformatycznych było zobowiązanie podmiotów realizujących zadania publiczne do realizowania okresowego audytu wewnętrznego, bez szczegółowego wskazywania na rodzaj audytu oraz tryb jego przeprowadzania.

KONTROLE NIK

W maju 2019r NIK przeprowadził szereg kontroli pod kątem bezpieczeństwa danych. Poddane zostały weryfikacji bezpieczeństwo danych w urzędach gmin, miast i starostwach. W opinii NIK, "nie jest możliwe zapewnienie wysokiego poziomu ochrony danych osobowych bez zachowania właściwego bezpieczeństwa informacji w systemach informatycznych". Wnioski i wytyczne prezentuje NIK na swojej stronie internetowej.

W 2019r i 2020r NIK przeprowadził w szereg kontroli pod kątem ePUAP. Bezpieczeństwo informacji w oparciu o rozporządzenie KRI oraz wymóg audytu w ocenie NIK był kluczowy.

Wyniki kontroli:

UM Grajewo, z dnia 18.08.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Hajnówka, z dnia 18.08.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Augustów, z dnia 31.07.2020r. **- w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Knurów, z dnia 6.11.2020r. - dokument pokontrolny
UM Łomża, z dnia 31.07.2020r. - dokument pokontrolny
UM Myszków, z dnia 6.11.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UMiG Pszczyna, z dnia 12.10.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UMiG Czechowice-Dziedzice, z dnia 6.11.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UMiG Swarzędz, z dnia 24.07.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Oborniki, z dnia 13.10.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Śrem, z dnia 2.10.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Wolsztyn, z 10.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Białogard z dnia 2.11.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Gryfino z dnia 2.11.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Wałcz z dnia z 3.09.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Police z dnia z 4.11.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Aleksandrów Łódzki z dnia z 19.10.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Opoczno z dnia 12.10.2020r. - dokument pokontrolny
UM Długołęka z 10.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Oleśnica z dnia 21.10.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Zgorzelec z 10.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**
UM Oława z 10.2020r. - **w dokumencie pokontrolnym stwierdzono nieprawidłowości...**

Czy PAŃSTWA podmiot wypełnia co roku obowiązek przeprowadzenia audytu Bezpieczeństwa Informacji zgodnie z Rozporządzeniem KRI ? Zachęcamy do kontaktu. Wycena kosztów zlecenia jest bezpłatna.

Uzupełnieniem **audytu KRI** może być **audyt bezpieczeństwa danych osobowych** o którym mówi art. 24 i 32 RODO. Zlecenie przeprowadzenia obydwu audytów jest uzasadnione oraz korzystniejsze cenowo

OPIS USŁUGI AUDYTU

1. Audyt przeprowadzany jest na podstawie i zgodnie z wymaganiami Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie *Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012r. poz. 526)*.
2. Zasady przeprowadzenia proponowanego audytu oparte są na wytycznych zawartych w dokumencie „*Wspólne stanowisko Departamentu Informatyzacji MAiC i Departamentu Audytu Sektora Finansów Publicznych MF odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji*'
3. Proponowany audyt spełnia wymagania dotyczące wyboru osób prowadzących audyt w zakresie bezpieczeństwa informacji. Zgodnie z wytycznymi zawartymi w dokumencie „*Wspólne stanowisko ...*" , są to: odpowiednie kwalifikacje, doświadczenie, znajomość metodyki audytu w zakresie bezpieczeństwa informacji, a także niezależność od obszaru audytowanego.
4. Proponowany audyt sytemu bezpieczeństwa informacji, zgodnie z wytycznymi zawartymi w dokumencie „*Wspólne stanowisko ...*", będzie przeprowadzony w oparciu o 14 kryteriów zawartych w § 20 ust. 2 Rozporządzenia
5. Metodyka audytu polega na ocenie stanu przestrzegania wymagań Rozporządzenia w oparciu o Załącznik nr 1 do Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych (Ankieta dotycząca działania systemów teleinformatycznych używanych do realizacji zadań publicznych)
6. Ocena będzie dokonywana poprzez gromadzenie dowodów zgodności w postaci oględzin dokumentacji oraz odbierania oświadczeń składanych przez osoby poddane audytowi.
7. Na podstawie zebranych informacji, zakończenie audytu skutkuje przygotowaniem i przedstawieniem sprawozdania z audytu. W przypadku stwierdzenia obszarów wymagających doskonalenia, sprawozdanie zawierać będzie propozycje ewentualnych działań naprawczych.
8. Audyt obejmuje sprawdzenie wykonania obowiązków w zakresie :
   1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
   2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
   3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
   4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
   5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
   6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,

c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób,
umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

OFERUJEMY TAKŻE SZKOLENIA Z BEZPIECZEŃSTWA INFORMACJI I RODO

Spełnienie obowiązku z przeprowadzenia obligatoryjnego szkolenia z zasad bezpieczeństwa dla pracowników Państwa jednostki (na podst. § 20 ust. 2, pkt. 6 Rozporządzenia KRI) oraz szkolenia z zakresu ochrony danych osobowych(art. 39 ust.1 lit b RODO)

W sprawie organizacji audytu prosimy o kontakt:

EX LEGE SZKOLENIA PRAWNICZE, OUTSOURCING USŁUG IOD RAFAŁ ANDRZEJEWSKI
ul. Jurowiecka 19/147, 15-101 Białystok, NIP:9661722551
oddziały: Kraków, Poznań, Łódź, Rzeszów
Kontakt:
Rafał Andrzejewski
+48 504-976-690,
iod.r.andrzejewski@szkoleniaprawnicze.com.pl
Małgorzata Kuc-Wiśniewska
+48 784037658
ex.lege@szkoleniaprawnicze.com.pl

Anna Bułkowska
+48 511047472
ex.lege2@szkoleniaprawnicze.com.pl

Więcej na stronie: https://exlegeiod.pl/szkoleniaiod/