

Procedura audytu

Celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.

1. Administrator (ewentualnie IOD) jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej.
2. Administrator odpowiada za przeprowadzony audyt.
3. Administrator (ewentualnie IOD) opracowuje programy audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.
4. Administrator (ewentualnie IOD) jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów
5. Administrator (ewentualnie IOD) realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO.
6. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia
7. Wynik audytu zostaje udokumentowany przez Administratora (ewentualnie IOD).
8. Administrator dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.
9. Audyt jest przeprowadzany cyklicznie, nie rzadziej niż raz na rok. Administrator może zarządzić przeprowadzenie audytu doraźnego pełnego i częściowego.