

Analiza ryzyka i ocena skutków – wytyczne

Niniejszy dokument opisuje sposób przeprowadzania analizy ryzyka i oceny skutków dla ochrony danych, o których mowa w RODO.

Spis treści

1. Wstęp	1
2. Analiza ryzyka	1
3. Ocena skutków	2

1. Wstęp

1. Do przestrzegania zaleceń opisanych w niniejszym dokumencie zobowiązane są wszystkie osoby, współpracujące z ADO (niezależnie od stażu pracy, zajmowanego stanowiska lub podstawy współpracy), które w ramach obowiązków służbowych są zaangażowane w proces analizy ryzyka lub oceny skutków.
2. Analiza ryzyka lub ocena skutków jest dokonywana przez osobę lub osoby wyznaczone przez ADO, w ścisłej współpracy z IOD.
3. Analiza ryzyka lub ocena skutków dokonywana jest z uwzględnieniem:
 - 1) przepisów związanych z ochroną danych osobowych lub bezpieczeństwem informacji, w szczególności RODO,
 - 2) wskazówek Prezesa Urzędu Ochrony Danych Osobowych lub innego właściwego organu nadzorczego,
 - 3) metodologii innych organów zaangażowanych w ochronę danych osobowych, np. Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA).
4. Wyniki analizy ryzyka lub oceny skutków są przekazywane ADO w postaci odrębnych dokumentów.

2. Analiza ryzyka

1. Analiza ryzyka służy:
 - 1) ustaleniu, z jakim ryzykiem może wiązać się wykorzystanie danych osobowych w ramach czynności przetwarzania,
 - 2) stwierdzeniu, jakie działania powinny być podjęte przez ADO w celu zmniejszenia lub wyeliminowania ryzyka.
2. Analiza ryzyka jest dokonywana przez ADO dla wszystkich czynności przetwarzania, wyróżnionych w rejestrze czynności przetwarzania.
3. W celu dokonania ustaleń, o których mowa w ust. 1 powyżej, analizie podlegają w szczególności:
 - 1) potencjalne negatywne skutki przetwarzania danych osobowych w obszarze poufności, integralności i dostępności,
 - 2) obszary, w ramach których u ADO mogą wystąpić zagrożenia związane z ochroną danych osobowych i bezpieczeństwem informacji (zasoby sieciowe i techniczne; procedury przetwarzania danych osobowych; osoby lub podmioty zaangażowane w ochronę danych osobowych; zagrożenia sektorowe, skala działalności),

4. W celu dokonania ustaleń, o których mowa w ust. 1 powyżej, osoba odpowiedzialna za analizę ryzyka może żądać od osób współpracujących z ADO:
 - 1) składania ustnych wyjaśnień,
 - 2) przedkładania dokumentów,
 - 3) udostępniania informacji z systemów informatycznych, aplikacji, programów, sprzętów lub sieci ADO.
5. Na podstawie przeprowadzonej analizy określany jest poziom ryzyka, związany z czynnością lub czynnościami przetwarzania. W zależności od stwierdzonego poziomu ryzyka ADO podejmuje (ustalone we współpracy z IOD) działania minimalizujące ryzyka. Jeżeli przeprowadzona analiza ujawni wysoki poziom ryzyka związany z czynnością lub czynnościami przetwarzania, ADO dokonuje dodatkowo oceny skutków.
6. Analiza ryzyka jest dokonywana cyklicznie, nie rzadziej niż raz na rok kalendarzowy.

3. Ocena skutków

1. Oceny skutków ADO dokonuje:
 - 1) w razie stwierdzenia, że analiza ryzyka ujawni wysoki poziom ryzyka związany z czynnością lub czynnościami przetwarzania,
 - 2) w sytuacjach określonych RODO,
 - 3) dla operacji przetwarzania wskazanych w wykazie ogłoszonym przez Prezesa Urzędu Ochrony Danych Osobowych lub inny właściwy organ nadzorczy.
2. W ramach oceny skutków analizie podlegają w szczególności:
 - 1) sposób przetwarzania danych osobowych,
 - 2) konsultacja sposobu przetwarzania danych osobowych,
 - 3) adekwatność i proporcjonalność przetwarzania,
3. Na podstawie oceny skutków ustalane są:
 - 1) ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
 - 2) środki minimalizujące ryzyka naruszenia praw lub wolności osób, których dane dotyczą.
4. W celu dokonania analizy, o której mowa w ust. 2 powyżej, osoba odpowiedzialna za ocenę skutków może żądać od osób współpracujących z ADO:
 - 1) składania ustnych wyjaśnień,
 - 2) przedkładania dokumentów,
 - 3) udostępniania informacji z systemów informatycznych, aplikacji, programów, sprzętów lub sieci ADO.
5. Ocena skutków jest dokonywana cyklicznie, nie rzadziej niż raz na rok kalendarzowy.