Jak przeprowadzać analizę ryzyka zgodnie z zasadą rozliczalności?

Posted on 2026-01-30

RODO opiera się na zasadzie rozliczalności, zgodnie z którą administratorzy oraz podmioty przetwarzające są zobowiązani nie tylko do przestrzegania przepisów dotyczących ochrony danych osobowych, lecz także do wykazania, że realizują swoje obowiązki świadomie i adekwatnie wobec ryzyka naruszenia praw lub wolności osób, których dane przetwarzają. Analiza ryzyka odgrywa w tym mechanizmie kluczową rolę, stanowiąc podstawę do podejmowania decyzji dotyczących sposobu przetwarzania danych oraz doboru technicznych i organizacyjnych środków ich ochrony. Poniżej przedstawiamy listę 18 dobrych praktyk, które mogą pomóc w przeprowadzaniu analizy ryzyka w sposób zgodny z zasadą rozliczalności.

Ø

1.Stawiaj prawa i wolności człowieka w centrum analizy ryzyka

Ryzyko w rozumieniu RODO zawsze powinno być analizowane z perspektywy osoby, której dane dotyczą, a nie organizacji, która te dane przetwarza (np. przez pryzmat ryzyka

finansowego, wizerunkowego lub operacyjnego). Ma to szczególne znaczenie przy określaniu wagi skutków urzeczywistnienia się określonych zagrożeń.

Pomimo że perspektywa organizacji pozostaje istotna na etapie identyfikacji źródeł zagrożeń i podatności mogących prowadzić do naruszenia praw lub wolności jednostki, warto zachować właściwe rozróżnienie pomiędzy źródłem ryzyka a jego skutkami – które zawsze powinny być oceniane z punktu widzenia osób, których dane dotyczą.

Takie podejście jest niezbędne zarówno dla prawidłowego zarządzania ryzykiem, jak i dla wykazania, że analiza ryzyka została przeprowadzona zgodnie z celami RODO. Przykładem błędnej praktyki byłoby uznanie ryzyka za niskie wyłącznie dlatego, że potencjalne negatywne konsekwencje dotyczą niewielkiej liczby osób.

2.Odwołuj się do wymogów i wskazówek zawartych w RODO

Analiza ryzyka nie powinna być prowadzona w oderwaniu od przepisów RODO, lecz osadzona w kryteriach i wskazówkach w nim określonych (np. w art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1, art. 35 ust. 7 oraz motywach 74-76 i 83-84). W szczególności należy uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz prawdopodobieństwo i wagę potencjalnych konsekwencji dla praw lub wolności osób fizycznych.

W praktyce oznacza to konieczność odnoszenia analizy ryzyka do rzeczywistego kontekstu danego procesu, w tym do celów, w jakich dane są wykorzystywane, a nie wyłącznie do technicznego sposobu ich przetwarzania. Ten sam system lub narzędzie (np. rozwiązania oparte na sztucznej inteligencji) może się wiązać z różnym poziomem ryzyka w zależności od celu przetwarzania – innym, gdy służy do oceny kandydata do pracy, a innym, gdy wykorzystywany jest np. do porządkowania treści. Uwzględnienie tych kryteriów umożliwia wykazanie, że analiza została przeprowadzona w sposób świadomy, spójny i zgodny z zasadą rozliczalności.

3.Opieraj analizę ryzyka na faktach i dowodach, a nie na intuicji

Ocena ryzyka powinna wynikać z możliwie obiektywnych przesłanek. Każdą wartość – zarówno liczbową, jak i opisową – przypisywaną do poszczególnych parametrów oceny (np. prawdopodobieństwa wystąpienia zagrożeń lub wagi ich skutków) warto uprzednio zdefiniować i oprzeć na konkretnych przesłankach faktycznych lub technicznych, a nie wyłącznie na arbitralnych założeniach. W tym kontekście przydatne mogą się okazać uznane standardy, normy i metodyki (np. ISO).

Taka praktyka sprzyja wykazywaniu, że analiza ryzyka została przeprowadzona w sposób rzetelny i nie ma charakteru abstrakcyjnego ani wyłącznie deklaratywnego oraz pomaga porównywać wyniki analiz przeprowadzanych w różnych okresach.

4. Dokumentuj źródła ocen i przyjętych założeń

Podstawy, na których oparto analizę ryzyka, powinny być możliwe do zidentyfikowania i obejmować uznane normy techniczne, metodyki, wytyczne, doświadczenia organizacyjne lub inne materiały odnoszące się do znanych zagrożeń i dobrych praktyk. Ich dokumentowanie ma istotne znaczenie zwłaszcza w przypadku przyjmowania określonych założeń, uproszczeń lub skal ocen, które mają wpływ na wyniki analizy.

Ma to na celu umożliwienie odtworzenia toku wnioskowania administratora lub podmiotu przetwarzającego oraz wykazanie, że ryzyko zostało oszacowane na podstawie obiektywnych przesłanek.

5. Traktuj analizę ryzyka jako proces ciągły, a nie jednorazowe działanie

Analiza ryzyka nie ma charakteru jednorazowego „ćwiczenia”, lecz powinna być postrzegana jako proces towarzyszący przetwarzaniu danych osobowych. Wszelkie zmiany dotyczące przetwarzania mogą wpływać na charakter i poziom ryzyka, a tym samym powodować konieczność weryfikacji przyjętych uprzednio założeń. Sprzyja to utrzymaniu aktualności analizy oraz wykazywaniu, że administrator lub podmiot przetwarzający na bieżąco zarządza ryzykiem związanym z przetwarzaniem.

W związku z tym istotne jest, aby w organizacji istniały mechanizmy pozwalające osobom odpowiedzialnym za procesy biznesowe na identyfikację sytuacji, w których konieczne jest dokonanie ponownej analizy ryzyka. Może to dotyczyć w szczególności wprowadzenia nowych operacji na danych, modyfikacji zakresu przetwarzanych danych, pojawienia się nowych typów zagrożeń, włączenia do procesu nowych zasobów, zmiany osób odpowiedzialnych za przetwarzanie lub zmiany zasad dostępu i ujawniania danych. Mechanizmy te stanowią element zarządzania zmianą w organizacji i pozwalają powiązać analizę ryzyka z rzeczywistymi zmianami zachodzącymi w procesach przetwarzania.

6. Wersjonuj analizy ryzyka i dokumentuj istotne zmiany w ich treści

Dokumentowanie zmian w analizie ryzyka ma szczególne znaczenie w sytuacjach, w których modyfikowany jest sposób przetwarzania danych, stosowane środki ich ochrony lub inne istotne okoliczności towarzyszące procesom przetwarzania.

Wersjonowanie analiz ryzyka pozwala ustalić, jaka ocena obowiązywała w danym momencie oraz na jakiej podstawie były podejmowane określone decyzje. Ma to znaczenie dla wykazania ciągłości i spójności działań podejmowanych przez administratora lub podmiot przetwarzający, zwłaszcza w kontekście ich późniejszej weryfikacji.

7. Opisuj przetwarzanie w sposób kompletny, konkretny i zgodny z realiami

Analiza ryzyka powinna wiernie odzwierciedlać rzeczywisty sposób przetwarzania danych osobowych, a nie jego modelowy lub wyłącznie deklaratywny obraz. Należy więc opierać ją na faktach, uwzględniając wszelkie istotne elementy analizowanego procesu, w tym te, które mogą wpływać niekorzystnie (z perspektywy praw lub wolności osób fizycznych) na ostateczny poziom ryzyka.

W praktyce obraz przetwarzania może różnić się nie tylko ze względu na charakter przetwarzanych danych, ale również ze względu na podmioty, których dane dotyczą. W szczególności odmiennego podejścia wymaga przetwarzanie danych osobowych dzieci.

Nie należy także ograniczać analizy ryzyka do pojedynczego zasobu (np. systemu IT), z pominięciem szerszego kontekstu procesu przetwarzania, który ten zasób wspiera. Nie wyklucza to dokonywania analizy „dla zasobu" – szczególnie w zakresie identyfikacji zagrożeń – jednak bez zrozumienia procesów, które dany zasób wspiera, nie jest możliwe prawidłowe oszacowanie m.in. wagi potencjalnych negatywnych konsekwencji dla praw lub wolności osób fizycznych.

Tylko takie podejście pozwala zapewnić rzetelność analizy ryzyka oraz realną ochronę interesów osób, których dane dotyczą.

8. Analizuj cały cykl życia danych – od pozyskania do usunięcia

Analiza ryzyka powinna obejmować wszystkie etapy przetwarzania danych osobowych – od ich pozyskania, przez przechowywanie, wykorzystywanie i udostępnianie, aż po usunięcie lub anonimizację.

Ryzyka mogą się pojawiać na różnych etapach cyklu życia danych, również na etapie końcowym, np. w związku z błędami w anonimizacji. Pomijanie poszczególnych etapów lub traktowanie całego procesu jednolicie może prowadzić do nieprawidłowych wniosków, ponieważ poziom ryzyka oraz adekwatne środki ochrony danych mogą się istotnie różnić w zależności od etapu przetwarzania.

W praktyce istotne jest także zrozumienie, których zasobów dotyczą poszczególne operacje na danych oraz w jaki sposób są one realizowane. Identyfikacja operacji na danych stanowi punkt wyjścia do rozpoznania dalszych niuansów dotyczących przetwarzania, takich jak sposób realizacji operacji (np. lokalnie na urządzeniu użytkownika lub w ramach usługi chmurowej, w trybie ciągłym lub incydentalnym) czy częstotliwość ich wykonywania. Czynniki te mogą mieć bezpośredni wpływ na prawdopodobieństwo materializacji zagrożeń i powinny być uwzględniane w analizie ryzyka.

9. Uwzględniaj wszystkie zasoby wspierające proces, którego dotyczy analiza ryzyka

Analiza ryzyka powinna uwzględniać wszystkie zasoby zaangażowane w proces przetwarzania danych osobowych. Przede wszystkim dotyczy to osób uczestniczących w przetwarzaniu, stosowanych rozwiązań technicznych oraz procesów organizacyjnych, które mogą wpływać na sposób przetwarzania danych i poziom ryzyka. Pozwala to lepiej identyfikować rzeczywiste źródła zagrożeń oraz wykazywać, że analiza obejmuje pełny kontekst przetwarzania, a nie jedynie jego wybrane aspekty.

10. Nie ograniczaj analizy ryzyka do obszaru bezpieczeństwa danych (poufności, integralności i dostępności)

Analiza ryzyka nie powinna koncentrować się wyłącznie na zagrożeniach związanych z bezpieczeństwem danych, takich jak nieuprawniony dostęp, utrata czy zniszczenie.

Mimo że bezpieczeństwo informacji stanowi fundament ochrony prywatności, ryzyko dla praw lub wolności osób fizycznych może wynikać również ze sposobu przetwarzania danych, zwłaszcza w przypadkach profilowania, automatycznego podejmowania decyzji lub braku przejrzystości. Aspekty te mogą stanowić samodzielne źródła ryzyka i powinny być uwzględniane w analizie niezależnie od poziomu zabezpieczeń technicznych.

W szczególności w kontekście wykorzystywania systemów opartych na sztucznej inteligencji istotne jest zwrócenie uwagi na kwestie przejrzystości przetwarzania, poprawności i jakości danych oraz potencjalne konsekwencje podejmowania decyzji w sposób zautomatyzowany, w tym na bazie profilowania. Mechanizmy te mogą w znaczący sposób wpływać na sytuację osób, których dane dotyczą, nawet przy braku naruszeń ochrony danych osobowych w rozumieniu RODO.

11. Zwróć uwagę na mniej oczywiste, pośrednie i długofalowe skutki przetwarzania dla osób fizycznych

Analizując ryzyko, należy zwrócić uwagę nie tylko na bezpośrednie i natychmiastowe skutki przetwarzania danych, ale również na jego konsekwencje pośrednie lub ujawniające się w

dłuższym horyzoncie czasowym, w zakresie, w jakim mogą być one racjonalnie przewidziane. Uwzględnienie takich aspektów pozwala uniknąć zawężenia analizy wyłącznie do najbardziej oczywistych scenariuszy i lepiej odzwierciedlić rzeczywisty wpływ przetwarzania na sytuację osób, których dane dotyczą.

12. Uwzględniaj „stan wiedzy technicznej" oraz „koszt wdrażania" przy doborze środków ochrony danych

Przy doborze technicznych i organizacyjnych środków ochrony danych należy uwzględniać aktualny stan wiedzy technicznej oraz koszt ich wdrażania jako kryteriów pozwalających dopasować środki do specyfiki administratora lub podmiotu przetwarzającego oraz kontekstu przetwarzania. Kryteria te nie mogą jednak stanowić uzasadnienia dla kontynuowania przetwarzania danych pomimo istnienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Ich zastosowanie powinno pozostawać w bezpośrednim związku z wynikami analizy ryzyka i umożliwiać wykazanie zasadności przyjętych rozwiązań.

Stan wiedzy technicznej powinien być przy tym na bieżąco monitorowany, tak aby stosowane środki odpowiadały aktualnym zagrożeniom. W tym kontekście pomocne mogą być materiały publikowane przez wyspecjalizowane instytucje, takie jak ENISA, które w ramach cyklicznych raportów (np. „ENISA Threat Landscape") prezentują aktualne zagrożenia oraz przykładowe środki ochrony zgodne z obecnym stanem wiedzy technicznej.

13. Monitoruj wdrażanie zaplanowanych środków ochrony danych

Dobór środków ochrony danych powinien prowadzić do ich faktycznego wdrożenia i stosowania, a nie jedynie do formalnego wskazania ich w dokumentacji. Planowanie i monitorowanie wdrażania zaplanowanych środków pozwala potwierdzić, że decyzje podjęte w wyniku analizy ryzyka zostały rzeczywiście zrealizowane oraz że pozostają aktualne w świetle zmieniających się okoliczności towarzyszących przetwarzaniu. Ma to znaczenie zarówno dla skutecznej ochrony danych osobowych, jak i dla wykazania, że administrator

lub podmiot przetwarzający sprawuje rzeczywistą kontrolę nad realizacją przyjętych rozwiązań.

Dobrą praktyką jest także określenie ról i odpowiedzialności w zakresie faktycznego wdrażania zabezpieczeń, co ułatwia przypisanie działań do konkretnych osób lub komórek organizacyjnych oraz wspiera zapewnienie zgodności z zasadą rozliczalności.

14. Dokumentuj regularne testowanie skuteczności stosowanych zabezpieczeń

Wdrożenie określonych zabezpieczeń nie jest wystarczające, jeżeli nie towarzyszy mu mierzenie ich rzeczywistej skuteczności. Regularne testowanie środków bezpieczeństwa powinno umożliwiać ocenę, czy założenia przyjęte w ramach analizy ryzyka pozostają aktualne oraz czy stosowane rozwiązania spełniają swoje funkcje.

Dokumentowanie wyników takich testów pozwala wykazać, że administrator lub podmiot przetwarzający w sposób ciągły realizuje swoje obowiązki, monitorując bezpieczeństwo danych i podejmując adekwatne działania w celu ich bieżącej ochrony.

15. Jasno określ role i odpowiedzialność w procesie analizy ryzyka

Role i odpowiedzialności związane z zarządzaniem ryzykiem powinny być jasno określone i realizowane w praktyce, a nie ograniczać się do ogólnych zapisów w dokumentacji. W szczególności istotne jest wskazanie, kto odpowiada za przeprowadzenie analizy ryzyka, kto podejmuje decyzje dotyczące doboru adekwatnych środków ochrony danych oraz kto ostatecznie faktycznie wdraża je w organizacji. Przypisanie ról ma kluczowe znaczenie dla rozliczalności, ponieważ umożliwia ustalenie, na jakim etapie, przez kogo oraz na jakiej podstawie zostały podjęte określone decyzje.

16. Zapewnij realny udział inspektora ochrony danych w procesie oceny ryzyka

Udział inspektora ochrony danych w procesie analizy ryzyka powinien mieć charakter rzeczywisty i być możliwy do wykazania. Inspektor ochrony danych powinien być włączany

w proces analizy w zakresie odpowiadającym jego zadaniom i kompetencjom wynikającym z RODO, w szczególności w celu formułowania zaleceń, opiniowania przyjętych rozwiązań oraz monitorowania zgodności przetwarzania z przepisami o ochronie danych osobowych.

Jednocześnie odpowiedzialność za przeprowadzanie analizy ryzyka oraz za podejmowanie decyzji w jej następstwie pozostaje po stronie administratora lub podmiotu przetwarzającego. Zakres udziału inspektora ochrony danych, a także sposób uwzględnienia jego zaleceń lub przyczyny ich nieuwzględnienia powinny znajdować odzwierciedlenie w dokumentacji oraz w praktyce organizacyjnej.

17. Traktuj zatwierdzenie analizy ryzyka jako świadomą i udokumentowaną decyzję zarządczą

Zarządzanie ryzykiem w naturalny sposób prowadzi do sytuacji, w której pomimo zastosowania odpowiednich środków ochrony danych pewien poziom ryzyka dla praw lub wolności osób fizycznych nadal pozostaje. Decyzje dotyczące dalszego przetwarzania danych w takich warunkach powinny mieć charakter świadomy oraz być jednoznacznie przypisane do konkretnej osoby lub organu w ramach organizacji.

Niezależnie od przyjętych rozwiązań ostateczna odpowiedzialność za analizę ryzyka oraz jej konsekwencje zawsze spoczywa na administratorze lub podmiocie przetwarzającym.

18. Dokumentuj i uzasadniaj decyzje o odstąpieniu od dalszych działań związanych z zarządzaniem ryzykiem

Zasada rozliczalności obejmuje nie tylko działania podjęte w następstwie analizy ryzyka, lecz również decyzje o odstąpieniu od określonych działań. W szczególności dotyczy to rezygnacji z przeprowadzenia oceny skutków dla ochrony danych (DPIA), nieuwzględnienia rekomendacji inspektora ochrony danych lub niewdrożenia dodatkowych środków ochrony danych. Decyzje tego rodzaju powinny być udokumentowane i oparte na wynikach analizy, w sposób umożliwiający wykazanie, że zostały podjęte świadomie oraz z uwzględnieniem

ochrony praw i wolności osób fizycznych.

Podsumowanie

Analiza ryzyka w rozumieniu RODO nie jest celem samym w sobie ani jedynie formalnym obowiązkiem dokumentacyjnym. Stanowi ona proces, w ramach którego administrator lub podmiot przetwarzający podejmuje świadome decyzje dotyczące przetwarzania danych osobowych. Z perspektywy zasady rozliczalności kluczowe znaczenie ma nie tylko samo przeprowadzenie analizy, lecz również możliwość zapewnienia transparentności w zakresie źródeł przyjętych założeń, dokonanych ocen oraz podjętych decyzji (w tym decyzji o zaniechaniu określonych działań). Powyższe wskazówki mogą stanowić punkt odniesienia przy budowaniu rzetelnego, spójnego i możliwego do wykazania podejścia do realizacji obowiązków wynikających z przepisów o ochronie danych osobowych.