Z dziennika tłumaczki. Rozważania o RODO

Odcinek 13 - Analiza ryzyka

Poniedziałek 28 maja 2018 r., 3 dni po RODO

Drogi Dzienniku,

dzisiaj będzie o ryzyku. I prawdopodobieństwie wystąpienia wysokiego ryzyka. No właśnie, jak mogę ocenić ryzyko związane z przetwarzaniem danych osobowych i jak mogę ocenić prawdopodobieństwo wystąpienia ryzyka naruszenia praw i wolności osób, których dane przetwarzam?

Trudna sprawa. Gdybym miała ocenić prawdopodobieństwo, że moja sekretarka złamie rękę właśnie teraz, kiedy mam tyle pracy z przygotowaniami do RODO, to bym powiedziała, iż wynosi ono jeden na milion. No ale zdarzyło się, mimo że prawdopodobieństwo było bardzo małe, a skutki dotkliwe. Ale najgorsze, że tak naprawdę niewiele wpływu miałam na to wydarzenie.

Tak samo jest z ryzykiem związanym z przetwarzaniem danych osobowych. Do tej pory nie zdarzały mi się ryzykowne sytuacje, gdzie prawa i wolności osób byłyby zagrożone w związku z przetwarzaniem ich danych.

Ale … w zeszłym tygodniu zostawiłam klucze w drzwiach do biura. Chyba byłam tak rozkojarzona przez to rozporządzenie, że nie zauważyłam. Na szczęście klient grzecznie mi zwrócił uwagę i nic się nie stało. Jakieś ryzyko było, na przykład, że ktoś ukradnie mi komputer. Pytanie, jak duże było to ryzyko?

Jeżeli dobrze zabezpieczę dane, to w istocie ryzyko będzie niewielkie. Jednak jakieś będzie. Jakie zatem będzie prawdopodobieństwo, że dojdzie do naruszenia praw i wolności osób fizycznych? Jak mam to ocenić? Czy ja w ogóle muszę to oceniać?

W rozporządzeniu czytam tak:

> *Artykuł 35 Ocena skutków dla ochrony danych*
>
> *1. Jeżeli dany rodzaj* ***przetwarzania*** *– w szczególności z użyciem nowych technologii –* ***ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych****,* ***administrator*** *przed rozpoczęciem przetwarzania dokonuje* ***oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych****. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.*

2. (...)
3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest ***wymagana w szczególności*** *w przypadku:*
a) ***systematycznej, kompleksowej oceny czynników osobowych*** *odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;*
b) ***przetwarzania na dużą skalę*** *szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub*
c) ***systematycznego monitorowania*** *na dużą skalę miejsc dostępnych publicznie.*

Patrząc na ust. 3, dochodzę do wniosku, że moja działalność raczej nie wymaga przeprowadzania oceny skutków dla ochrony danych. W ust. 1 jest mowa o „dużym prawdopodobieństwie spowodowania ryzyka naruszenia praw i wolności osób fizycznych". W przypadku danych, które przetwarzam jako administrator raczej nie ma takiego prawdopodobieństwa, bo są to tylko dane kontaktowe i ewentualnie dane do faktury. I tylko w tym zakresie jako administrator musiałabym przeprowadzić taką ocenę. W tym wypadku ocena raczej mnie nie dotyczy.

Na wszelki wypadek chciałabym jednak ustalić, czy przetwarzanie, którego dokonuję może z dużym prawdopodobieństwem spowodować wysokie ryzyko naruszenia tych praw i wolności. Na własny użytek i dla spokoju ducha, a także do mojej dokumentacji, w razie gdyby ktoś zapytał, czy jestem dobrze przygotowana.
Nawet jeżeli moje przetwarzanie w charakterze administratora nie kwalifikuje się pod obowiązek przeprowadzenia oceny skutków, to jednak warto oszacować prawdopodobieństwo wystąpienia ryzyka jako podstawę do wdrożenia odpowiednich środków organizacyjnych i technicznych. Niezależnie bowiem od tego, czy przetwarzam dane osobowe w charakterze administratora czy podmiotu przetwarzającego muszę wdrożyć odpowiednie środki bezpieczeństwa. Ale o tym później.

Najpierw zrobię taką małą analizę ryzyka (nie nazwę tego oceną skutków, bo przecież stwierdziłam, że oceny skutków nie muszę wykonywać).

W mojej analizie uwzględnię charakter, zakres, kontekst i cele przetwarzania. Podstawą analizy będzie już przygotowana tabelka z procesami i zbiorami danych. Tam mam już zakres i cele przetwarzania, kontekst też, bo jest podane, w ramach jakiej działalności ma ono miejsce oraz gdzie dane są przechowywane.

Teraz pytanie, jakie ryzyko jest związane z tymi czynnikami? W komentarzu Becka (str. 447) autorzy proponują skalę: brak ryzyka - (zwykłe) ryzyko - wysokie ryzyko

- charakter i zakres danych:
    - dane, które przetwarzam jako administrator są zwykłymi danymi = zwykłe ryzyko (bo zawsze jakieś ryzyko jest);
    - dane, które przetwarzam jako podmiot przetwarzający lub działając z upoważnienia mogą być wrażliwymi danymi = zwykłe albo wysokie ryzyko;
- cele i wykonane czynności przetwarzania: zwykłe ryzyko (nie zmieniam danych, nie interpretuję, nie używam ich do tworzenia nowych dokumentów, nie profiluję nikogo na podstawie danych);
- kontekst i miejsce przechowywania danych: zwykłe ryzyko po wdrożeniu odpowiednich środków technicznych.

W artykule 32 dotyczącym bezpieczeństw przetwarzania czytam jeszcze:

> *Artykuł 32 Bezpieczeństwo przetwarzania*
> *2.Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności* ***ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych****.*

Dopiszę do mojej oceny taką ładną formułkę, zawierającą te informacje. W pliku z dokumentacją już przygotowałam wszystko do oceny, ale muszę jeszcze uzupełnić poszczególne rubryczki.

Ryzyko jest - wysokie i niskie, diagnoza postawiona. Teraz trzeba coś zrobić z pacjentem: działania profilaktyczne, leczenie zachowawcze czy radykalny zabieg chirurgiczny?

Jutro zrobię rozpiskę środków technicznych i organizacyjnych zalecanych przez specjalistów od RODOzy.
Papa!
Twoja Tłumaczka