Warszawa, 16.06.2020 r.

Analiza ryzyka w procesach przetwarzania

W raporcie Związku Firm Ochrony Danych Osobowych[1], w którego powstaniu iSecure brała aktywny udział, brak analizy ryzyka wskazano jako jeden z 10 największych błędów przy zapewnianiu zgodności z RODO.

Czym jest analiza ryzyka?

Mówiąc obrazowo, analiza ryzyka to sprawdzenie wszystkich procesów przetwarzania danych osobowych i oszacowanie, jakie ryzyka występują w danym procesie na czas sprawdzenia. Przez „ryzyka" rozumiemy ryzyko naruszenia praw lub wolności osób, których dane są przetwarzane (np. prawo dostępu do danych, prawo uzyskania pełnej informacji o przetwarzaniu danych, zachowanie poufności danych). Wynikiem analizy ryzyka powinna być wiedza w firmie, które procesy lub elementy procesów generują ryzyko naruszeń, ale też jak te ryzyka wyeliminować lub zminimalizować.

Jak przeprowadzić analizę ryzyka?

Okazuje się, że wiele firm albo nie ma w ogóle przeprowadzonej oceny ryzyka dla posiadanych zasobów, albo przeprowadzona ona została błędnie (np. przez niewykwalifikowany personel, czy z pominięciem niektórych ważnych elementów z powodu braku odpowiedniej świadomości czy doświadczenia w sprawdzanym obszarze). Pojawia się w takim momencie pytanie: „Jak dobrze przeprowadzić analizę ryzyka?"

Przede wszystkim, zgodnie z przemyślaną metodyką, czyli sposobem, modelem jej przeprowadzenia. Nie ma jednego obowiązującego modelu, w oparciu o który firmy muszą przeprowadzić ocenę ryzyka, dlatego istnieje pewien margines swobody w wypracowaniu ostatecznego kształtu przeprowadzanej analizy. Konkretna metodyka oceny ryzyka w danym podmiocie powinna uwzględniać jednak określone kryteria oceny, czyli wyróżnienie składników oceny ryzyka. W przypadku różnych podmiotów mogą być one odmienne, jednak są elementy wspólne:

- ocenę ryzyka przeprowadza się w odniesieniu do praw lub wolności osób, których dane dotyczą
- ocena weryfikuje, jak dane ryzyko wpływa na prawa czy wolności osób fizycznych
- ryzyka są definiowane, wskazywane, określane
- ocena szacuje szansę na wystąpienie danego ryzyka (ze względu na jego prawdopodobieństwo, podatność, itp.)
- ocena wskazuje, jakie środki bezpieczeństwa podjąć, aby zminimalizować ryzyko

Na podstawie tych elementów wspólnych ważne jest zatem, aby badając ryzyko wziąć pod uwagę między innymi:

- **konkretny proces**, czynność przetwarzania danych (np. na bazie rejestru czynności czy rejestru kategorii czynności przetwarzania danych)
- wyczerpującą **listę ryzyk**, które chcemy sprawdzać w każdym analizowanym procesie (w tym miejscu można posiłkować się ryzykiem niezgodności z obowiązkami wynikającymi z RODO,

[1] https://www.zfodo.org.pl/wp-content/uploads/2020/05/10-najwiekszych-bledow-przy-wdrazaniu-RODO.pdf

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

dotyczącymi kwestii formalnych, organizacyjnych, czy zabezpieczeń technicznych)

- oszacowanie, czy a jeżeli tak, to **w jakim stopniu konkretne ryzyko występuje w danym procesie**, przypisując mu odpowiednią wartość (np. w skali od 1 do 5, przy czym 1 oznaczałoby, że ryzyko jest nieprawdopodobne, a 5, że jest prawie pewne)
- oszacowanie, czy a jeżeli tak, to **w jakim stopniu konkretne ryzyko wpływa na naruszenie praw lub wolności** osób, których dane są przetwarzane (np. w skali od 1 do 5, przy czym 1 oznaczałoby, że nie ma żadnego wpływu, a 5, że ten wpływ jest bardzo istotny)
- w przypadku, gdy istnieje duże ryzyko (tj. o dużym prawdopodobieństwie wystąpienia i dużym wpływie na prawa i wolności osób) – wskazanie planu działań naprawczych, czyli zaleceń wdrożenia środków, które obniżą poziom ryzyka.

Wynikiem analizy ryzyka są m. in.:

- oszacowanie **poziomu ryzyka** znanego na dzień przeprowadzenia oceny ryzyka dla danego procesu
- odpowiedni dla oszacowanych ryzyk **wykaz działań, jakie należy podjąć, aby poziom ryzyka obniżyć**
- w przypadku **ryzyka akceptowalnego – potwierdzenie decyzji o jego zachowaniu**
- w przypadku **braku ryzyka – stwierdzenie braku konieczności podjęcia dalszych działań**

Przeprowadzenie analizy ryzyka nie jest łatwe. Same też wyniki końcowe, o których mowa powyżej mogą być uzyskiwane w różny sposób, zależny od przyjętej metodyki (np. poprzez sumowanie lub mnożenie wartości analizowanych w danym procesie, np. wartość prawdopodobieństwa wystąpienia ryzyka pomnożona przez wartość wpływu tego ryzyka na prawa i wolności da wynik końcowy poziomu ryzyka obecnego).

Warto zatem przede wszystkim najpierw przemyśleć, zaplanować metodę szacowania ryzyka, a następnie tej metody konsekwentnie się trzymać przeprowadzając ocenę.

Pamiętajmy przy tym, że RODO wymaga, aby dane osobowe zabezpieczyć odpowiednio do poziomu ryzyka, jaki wiąże się z ich przetwarzaniem. Aby wykazać zatem te adekwatne zabezpieczenia należy przede wszystkim znać ryzyka, w kontekście których zabezpieczenia są wdrażane. Dlatego analiza ryzyka jest bardzo istotnym elementem wdrożenia i należy ją przeprowadzić umiejętnie.

Przykłady elementów oceny ryzyka

Na przykładzie przedstawionych powyżej elementów wspólnych, jakie powinny się znaleźć w analizie ryzyka, poniżej znajduje się kilka praktycznych rozwiązań obrazujących **elementy wyjściowe** do oszacowania ryzyka. Samo jednak oszacowanie wyniku ryzyka, czyli podanie określonej wartości końcowej, byłoby karkołomnym zadaniem. Nawet gdyby pokusić się o wyprowadzenie określonego wyniku końcowego, to bazowałby on tylko na konkretnym, określonym schemacie oceny, który może być odmienny w organizacji X, niż stosowany w innej organizacji Y. Dlatego poniżej podajemy jedynie dane źródłowe, które być może pozwolą czytelnikom wykorzystać je i zastosować według własnej metody.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

Badany proces: Rekrutacja

Jakie jest ryzyko?	Na jakie prawa/wolności wpływa?	Jaki jest stopień wpływu tego ryzyka na to prawo/wolność (1-5)?	Jak bardzo prawdopodobne jest wystąpienie tego ryzyka (1-5)?	Środki bezpieczeństwa do wdrożenia
Brak tworzenia kopii zapasowych dysków laptopów	Brak skorzystania z praw dostępu do danych w przypadku utraty danych z dysku	5	2	Oprogramowanie automatycznie wykonujące kopię zapasową danych
Brak zabezpieczeń urządzeń mobilnych	Utrata poufności danych może powodować dotkliwe konsekwencje, jak np. próby wyłudzenia danych	5	1	Dodatkowe oprogramowanie umożliwiające zdalne zablokowanie dostępu lub wymazanie pamięci

Jakie jest ryzyko?	Na jakie prawa/wolności wpływa?	Jaki jest stopień wpływu tego ryzyka na to prawo/wolność (1-5)?	Jak bardzo prawdopodobne jest wystąpienie tego ryzyka (1-5)?	Środki bezpieczeństwa do wdrożenia
Brak zabezpieczenia dokumentacji papierowej przed jej przypadkową utratą lub zniszczeniem	Brak realizacji praw dostępu do danych lub niezałatwienie sprawy w przypadku zniszczenia lub zniekształcenia jedynego egzemplarza dokumentu	5	3	Wprowadzenie danych do systemu, sporządzenie kopii elektronicznej (skanu)
Brak oprogramowania antywirusowego na komputerze	Brak realizacji praw dostępu, wysokie ryzyko nieuprawnionego wykorzystania danych	5	3	Zainstalowanie oprogramowania przed rozpoczęciem przetwarzania danych

Jakie jest ryzyko?	Na jakie prawa/wolności wpływa?	Jaki jest stopień wpływu tego ryzyka na to prawo/wolność (1-5)?	Jak bardzo prawdopodobne jest wystąpienie tego ryzyka (1-5)?	Środki bezpieczeństwa do wdrożenia
Utrata poufności i dostępności danych spowodowana atakiem socjotechnicznym	Wysokie ryzyko nieuprawnionego wykorzystania danych – np. kradzież tożsamości	5	5	Przeszkolenie pracowników, wdrożenie procedury bezpiecznego korzystania z poczty elektronicznej i sieci
Kradzież laptopa	Wysokie ryzyko nieuprawnionego ich wykorzystania – np. kradzież tożsamości, upublicznienie danych, narażenie na stres	5	4	Szyfrowanie dysku twardego laptopa

Katarzyna Ułasiuk, iSecure Sp. z o.o.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł