# Uwzględnianie ochrony danych w fazie projektowania



**RAPORTY MrR**
**OCHRONA DANYCH**

**Krzysztof Mystek – Ekspert ochrony informacji, Uniwersytet Śląski**

Począwszy od 25 maja 2018 r. rozpocznie się okres stosowania ogólnego rozporządzenia o ochronie danych (dalej: r.o.d.o.)[1] . Celem tego aktu prawnego jest dostosowanie obowiązujących przepisów do wymogów otaczającej nas rzeczywistości. W założeniu powinien on regulować kwestie związane z ochroną prywatności[2] przez około dwie kolejne dekady[3], co odpowiada długości stosowania ustępującej powoli Dyrektywy 95/46/WE[4]. Zasadniczo r.o.d.o. nie stanowi rewolucji rozumianej jako odejście od wypracowanych podstawowych standardów. Jest ono raczej ewolucją, która wprowadza nowości mające odpowiadać na nowe zapotrzebowania. Forma rozporządzenia i wynikająca z tego tytułu jego bezpośrednia stosowalność jest jednak nową jakością. Ma ona na celu zharmonizowanie prawa dotyczącego ochrony danych osobowych na terenie Unii Europejskiej. Ten cel, jak się wskazuje, nie zostanie osiągnięty w pełni ze względu na dużą możliwość prawodawców krajowych do wydawania własnych przepisów. Jest to jednak konsekwencja wynikająca z różnic w porządkach prawnych poszczególnych państw członkowskich Unii Europejskiej.

Jednym z rozwiązań wprowadzanych przez r.o.d.o. jest uwzględnianie ochrony danych osobowych w fazie projektowania (*data protection by design*). Jest to novum pod względem bezpośredniego wyrażenia tej zasady w regulacji prawnej. Nie jest to jednakże rzecz całkowicie nieznana patrząc z perspektywy doktryny, czy też praktycznego stosowania aktualnych przepisów. Należy bowiem zwrócić uwagę, iż również obecnie na etapie rozpoczęcia przetwarzania danych musi ono być w pełni zgodne z odpowiednimi regulacjami. *Data protection by design* nie zawiera w sobie jednak jedynie krótkiego przesłania, aby odpowiednio wcześnie planować działania. Opiera się, w szerszym znaczeniu, na kompleksowym i wnikliwym spojrzeniu na cały proces prowadzenia działalności związanej z przetwarzaniem danych osobowych. Rozwijaniem tej koncepcji, określanej jako ochrona prywatności w fazie projektowania (*privacy by design*), zajmuje się od lat Ann Cavoukian[5] – była komisarz ds. informacji i ochrony danych prowincji Ontario w Kanadzie. Ochrona prywatności w fazie projektowania stała się również przedmiotem rezolucji podjętej na 32 Międzynarodowej Konferencji Rzeczników

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)(Dz.U.UE.L.2016.119.1).

[2] Prywatność jest poniekąd pojęciem szerszym od ochrony danych osobowych, niemniej jednak na potrzeby niniejszego artykułu rozróżnianie tych pojęć jest niecelowe.

[3] Opinia Europejskiego Inspektora Ochrony Danych nr 3/2015 z 28 lipca 2015 r., Wielka szansa dla Europy.
Zalecenia EIOD dotyczące możliwości reformy ochrony danych w UE (wraz z dodatkiem), s. 10, tekst dostępny pod adresem: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_PL.pdf [odczyt: 27.12.2016 r.].

[4] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U.UE.L.1995.281.31 ze zm.).

[5] Patrz np.: A. Cavoukian, Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices, Maj 2010, tekst dostępny pod adresem: http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf [dostęp: 27.12.2016 r.]

Ochrony Danych Osobowych i Prywatności w Jerozolimie w dniach 27-29.10.2010 r.[6]. W rezolucji tej przyjęto następujące zasady, którymi należy się kierować:

- Podejście proaktywne, nie reaktywne, i zaradcze, nie naprawcze,
- Prywatność jako ustawienie domyślne,
- Prywatność włączona w projekt,
- Pełna funkcjonalność: suma dodatnia, nie suma zerowa,
- Ochrona od początku do końca cyklu życia informacji,
- Widoczność i przejrzystość,
- Poszanowanie dla prywatności użytkowników[7].

Powyższe wypracowane zasady, choć ujęte w rezolucji miały walor doktrynalny, posiadają obecnie swe odzwierciedlenie w przepisach r.o.d.o. Na podstawie art. 25 ust. 1 r.o.d.o. administrator[8] jest bowiem zobowiązany do wdrażania odpowiednich środków technicznych i organizacyjnych, tak by spełnić wymogi rozporządzenia oraz chronić prawa osób, których dane dotyczą. Kluczowe w perspektywie niniejszego artykułu jest wskazanie, iż administrator powinien dokonywać takich czynności zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania. W praktyce oznacza to, że przed dokonaniem pierwszych czynności przetwarzania administrator jest zobowiązany do uwzględnienia i zaplanowania kwestii związanych z ochroną danych osobowych. Projektując produkt lub usługę należy więc mieć na uwadze to, w jaki sposób zapewnione zostanie prawidłowe stosowanie r.o.d.o. Należy w takim przypadku uwzględnić:

a) stan wiedzy technicznej,
b) koszt wdrażania,
c) charakter, zakres, kontekst i cele przetwarzania,
d) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania[9].

Ochrona danych jako ustawienie domyślne (*data protection by default*) polega na zastosowaniu takich środków technicznych oraz organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania[10]. Brak aktywności osoby, której dane dotyczą, nie może mieć dla niej skutków pod postacią obniżenia poziomu ochrony jej prywatności. Informacje nadmiarowe, naruszające zasadę minimalizacji danych, nie powinny być w ogóle zbierane. Podobnie należy odnieść się do danych, które stały się zbędne wraz z upływem czasu i realizacją, bądź dezaktualizacją, poszczególnych celów.

Należy zwrócić uwagę, że jedną z proponowanych metod osiągnięcia odpowiedniego poziomu bezpieczeństwa jest dokonanie jak najszybszej pseudonimizacji[11]. Stanowi ona, zgodnie z r.o.d.o., przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej[12]. W praktyce mamy do czynienia więc ze zbiorem informacji, które traktowane w izolacji mogłyby zostać uznane za anonimowe. Administrator posiada jednakże odpowiedni zestaw dodatkowych danych, które pozwalają na identyfikację poszczególnych osób. Pozwolić to może na ograniczenie ewentualnych skutków niepowołanego dostępu do danych osobowych. Warunkiem jest oczywiście, by dodatkowe informacje potrzebne do identyfikacji osób pozostały bezpieczne. Ponadto niektóre czynności przetwarzania nie wymagają operowania na zestawie danych dotyczących osób bezpośrednio zidentyfikowanych.

Nie należy zapominać, że uwzględnianie ochrony danych w fazie projektowania polega nie tylko na stosowaniu odpowiednich zabezpieczeń przed niepożądaną ingerencją, lecz również na zapewnieniu przejrzystości przetwarzania wobec osoby, której dane dotyczą. Przejawia się to przykładowo w realizacji obowiązków informacyjnych leżących po stronie administratora[13]. Konieczne jest także zapewnienie omawianym osobom możliwości skutecznego realizowania ich pozostałych praw[14]. Już w fazie projektowania systemów przetwarzania danych należy więc uwzględniać sposób, w jaki obowiązki administratora będą realizowane.

Ogólne rozporządzenie o ochronie danych zakłada, że należy zachęcać wytwórców „produktów, usług i aplikacji, by podczas opracowywania i pro-

[6] https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf [data odczytu: 18.12.2016 r.].

[7] Przyjęto tłumaczenie zgodne z projektem rezolucji dostępnym na stronie GIODO: http://www.giodo.gov.pl/1520084/id_art/3830/j/pl/ [data odczytu: 18.12.2016 r.].

[8] Zgodnie z art. 4 pkt 7 r.o.d.o. termin "administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

[9] Art. 25 ust. 1 r.o.d.o.

[10] Art. 25 ust. 2 r.o.d.o.

[11] Motyw 78 r.o.d.o.

[12] Art. 4 pkt 5 r.o.d.o.

[13] Art. 13 oraz 14 r.o.d.o.

[14] Np. art. 15 do 22 r.o.d.o.

jektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych”[15]. Przy projektowaniu produktów oraz usług konieczne jest myślenie o ochronie prywatności zwłaszcza tam, gdzie przetwarzanie są tzw. dane wrażliwe. Do tej kategorii z pewnością zaliczamy informacje związane np. ze stanem zdrowia pacjenta. Należy zauważyć, że ze stosowania rozporządzenia rozliczany będzie administrator danych (ewentualnie podmiot przetwarzający), nie zaś wytwórca. Trudno jednak spodziewać się, aby zwolenników zyskiwały niedostosowane do przepisów produkty oraz usługi.

Prywatność włączona w projekt oraz pełna funkcjonalność (suma dodatnia), to komplementujące się zasady. Mowa w tym przypadku o uwzględnianiu prywatności od początku oraz o projektowaniu systemów przetwarzania danych w taki sposób, aby osiąganie zamierzonych celów następowało wraz z poszanowaniem prywatności użytkowników. Zachowanie zgodności przetwarzania danych osobowych z prawem nie ma być przeszkodą i utrudnieniem, lecz powinno stanowić podstawowy element w pełni funkcjonalnego oraz bezpiecznego systemu. Konieczne jest myślenie, które charakteryzuje się orientacją na osiąganie obydwu tych założeń jednocześnie[16]. Należy odrzucić więc wybór polegający albo na zachowaniu prywatności, albo na osiągnięciu pełnej funkcjonalności.

Im bardziej zaawansowany sprzęt lub usługa, tym istotniejsza staje się dbałość o kwestie bezpieczeństwa oraz prywatności. Ma to miejsce zwłaszcza, jeżeli nowoczesne urządzenia mają za zadanie funkcjonować w powiązaniu z całym ekosystemem informatycznym. Złożone oraz bezpieczne systemy przetwarzania danych wymagają skrupulatnego przemyślenia założeń, na bazie których będą funkcjonowały. Stwarza to zapotrzebowanie na stosowanie takich koncepcji jak uwzględnianie ochrony danych w fazie projektowania. Obecna gospodarka w dużej mierze rozwija się dzięki przetwarzaniu informacji. Kluczem jest więc opanowanie sztuki efektywnego osiągania założonych celów w bezpieczny oraz zgodny z prawem sposób.

[15] Motyw 78 r.o.d.o.

[16] Patrz np: A. Cavoukian, K. El Emam, A Positive-Sum Paradigm in Action in the Health Sector, Marzec 2010, s. 1, tekst dostępny pod adresem: http://www.ontla.on.ca/library/repository/mon/24003/300358.pdf [dostęp: 27.12.2016 r.]; patrz też: motyw 6 r.o.d.o.