

**Paweł Walczak**  
**Microsoft**

## **„Praktyczne podejście do realizacji wymagań RODO w systemach teleinformatycznych”**

Zaadresowanie wymagań stawianych przez RODO powoduje konieczność wprowadzenia wielu nowych rozwiązań organizacyjnych uzupełnionych wsparciem odpowiednich mechanizmów technicznych służących do zarządzania danymi i zapewnienia ich bezpieczeństwa. W wystąpieniu chciałbym skupić się na tym drugim aspekcie, środkach technicznych, umożliwiających właściwą ochronę danych osobowych.

### **Niezaprzeczalność dostępu**

Kluczowym elementem ochrony danych jest niezaprzeczalność dostępu do danych i usług. Bezpieczeństwo dostępu do danych przestało opierać się na fizycznej ochronie miejsc ich składowania. Obecnie ochrona ta bazuje głównie na uprawnieniach dostępu do danych - niezależnie od miejsca, w którym się znajdują. Takie podejście wymaga stworzenia cyfrowych tożsamości wszystkich użytkowników, odpowiedniego ich zabezpieczenia i zapewnienia nadawania uprawnień dostępu opartych na rolach wraz ze ścieżkami akceptacji tych uprawnień. Ważnym elementem jest synchronizacja wszystkich źródeł tożsamości użytkownika w przypadku braku możliwości posługiwania się jednym zestawem poświadczeń tożsamości.

Składnikami takich mechanizmów jest usługa LDAP – najczęściej Active Directory oraz system zarządzania tożsamością – np. Microsoft Identity Manager.

### **Klasyfikacja danych**

Następnym elementem ekosystemu ochrony danych jest ich klasyfikacja, pozwalająca określić jakie dane generujemy i posiadamy, gdzie się one znajdują i kto ma do nich dostęp. Przystępując do klasyfikacji danych musimy zająć się dwoma obszarami ich przetwarzania, to znaczy klasyfikacją w trakcie tworzenia zbiorów danych (czy plików je zawierających) oraz klasyfikacją już posiadanych oraz pobieranych z zewnątrz danych.

Dobrym przykładem narzędzia pozwalającego przypisać danym odpowiednie etykiety (predefiniowane dla całej organizacji) jest usługa Azure Information Protection (AIP). Pozwala ona na opisanie zawartości dokumentów i wiadomości poczty elektronicznej tworzonych w składnikach pakietu biurowego Office 365. Uprawnieni administratorzy usługi mogą wymusić opisywanie każdego nowego dokumentu odpowiednią predefiniowaną etykietą. AIP może proponować właściwą klasyfikację wyszukując w tworzonym tekście typowe predefiniowane wzorce, takie jak PESEL, nr. dowodu osobistego, czy nr. karty kredytowej.

Ważną funkcją AIP jest też możliwość przeszukiwania zawartości plików przechowywanych w repozytoriach i systemach plików zgodnie z założonymi wzorcami i nadawania plikom odpowiednich etykiet klasyfikujących.

Innym, lecz podobnym w skutkach działania narzędziem jest SQL Data Discovery and Classification pozwalającym na wykrywanie określonych typów zawartości, klasyfikację, etykietowanie i raportowanie.

## **Szyfrowanie danych**

Szyfrowanie danych z nadawaniem odpowiednich uprawnień dostępu dla użytkowników, grup użytkowników i ról w systemach, jest klasyczną metodą zabezpieczającą dane niezależnie od miejsca w którym się znajdują. Największym problemem jest dostarczenie intuicyjnych lub wręcz automatycznych prostych w obsłudze narzędzi szyfrowania.

Przykładem skutecznego rozwiązania jest automatyzacja szyfrowania nowych dokumentów za pomocą Azure Rights Management współdziałające z AIP. Tworząc nowy dokument lub wiadomość użytkownik musi wybrać odpowiednią klasyfikację (np. „tajemnica przedsiębiorstwa” lub „dane osobowe”), a AIP powoduje automatyczne szyfrowanie takiej informacji z nadaniem odpowiedniego poziomu uprawnień dla odbiorców.

Zastosowanie powyżej opisanych, prostych w użyciu mechanizmów jest pierwszym, ale też niezbędnym krokiem przy wprowadzaniu zasad ochrony danych osobowych.

Dalsze działania nie są bez nich możliwe.