Warszawa, 08.07.2020 r.

Co było pierwsze, proces czy cel?

W świecie ciągłej rywalizacji o klienta, zmieniających się przepisów i powstawaniu nowych technologii odmieniających nasz styl życia, które mają na celu polepszyć nam jego jakość, przedsiębiorcy muszą mierzyć się z ciągłą modyfikacją procesów, adaptacją i tworzeniem nowych usług. Mając na uwadze, jak wiele decyzji musi zostać podjętych przez biznes i jak szybko trzeba reagować na wahania rynku, dla wielu spółek skutkuje to podejmowaniem błędnych decyzji, wdrożeniem rozwiązań, które nie przynoszą zamierzonych skutków, bądź w najgorszym przypadku skutkujących kosztami lub utratą wizerunku. Przedsiębiorstwa często bez zastanowienia, impulsywnie rozpoczynają korzystanie z technologii, które według reklamy mają zwiększyć efektywność lub bezpieczeństwo spółki. I tak wprowadza się monitoring biometryczny lub skanery odcisków palców, pomimo braku konieczności czy zasadności stosowania tak rozbudowanych systemów prewencji w danej sytuacji, np. ze względu na brak poufnej dokumentacji w pomieszczeniach objętych tego typu środkami bezpieczeństwa. Na gruncie przepisów i zasad ochrony danych osobowych należy zadać sobie jedno istotne pytanie: Co w spółce wystąpiło i występuje jako pierwsze? Proces związany z przetwarzaniem danych osobowych, czy cel, do którego spółka zmierza?

Najistotniejszym aspektem, który należy poruszyć w celu udzielenia odpowiedzi na to pytanie, jest aspekt historyczny. Przed wejściem w życie RODO istniały pewne przepisy zobowiązujące do przestrzegania zasad ochrony danych osobowych, które można przełożyć na działania w ramach zaprojektowania procesu z uwzględnieniem oznaczenia celu przetwarzania danych. Dzisiaj takie działania są elementem zasady “privacy by design”. Dowodem przemawiającym za istnieniem obowiązku wyznaczania “celu” przed rozpoczęciem procesu przetwarzania była konieczność rejestracji zbiorów (baz) danych u Generalnego Inspektora Ochrony Danych Osobowych (GIODO – ówczesny organ nadzorczy). Rejestracja zbiorów danych wymagała analizy ich zawartości. Oznacza to, że w przypadku wprowadzania jakichkolwiek kluczowych zmian w przeznaczeniu bazy danych, zachodziła konieczność ustalenia celu i zakresu nowych działań, aby prawidłowo wykonać obowiązek aktualizacji rejestru zbiorów w GIODO. W odróżnieniu od masowego stosowania RODO, wiele przedsiębiorstw w Polsce przed wejściem w życie RODO nie przestrzegało polskich przepisów, które obowiązywały od 1997 roku. Powodów może być wiele, ale jako jeden z nich można wskazać znacznie mniejszy rygor kary za nieprzestrzeganie przepisów w porównaniu do tej, od która wynika z przepisów RODO. Innym powodem mogła być także niska egzekwowalność stosowania polskich przepisów.

Cel przetwarzania, zasada minimalizacji jak i ograniczenie czasowe przetwarzania danych z chwilą wejścia w życie RODO były nowością dla wielu administratorów danych osobowych, mimo tego, że zasady te istniały w Polsce od czasu stosowania poprzedniej ustawy o ochronie danych osobowych (a więc od 1997 roku). Jeden z pierwszych obowiązków dla nowo powołanych IOD w wielu spółkach polegał na wykryciu wszystkich występujących w spółce procesów przetwarzania i na tej podstawie przyporządkowanie celów lub zarekomendowanie zaniechania określonych działań. Brak celów i kontroli nad procesami był widoczny w przedsiębiorstwach najczęściej w toku tworzenia pierwszej wersji rejestru czynności przetwarzania danych.

Drugim istotnym aspektem jest świadomość. Zasada "privacy by design" jest dla wielu administratorów całkowitą nowością. W chwili obecnej przestrzeganie powyższej zasady jest uznawane przez większość biznesu jako kolejna procedura spowalniającą prowadzenie procesów. W spółkach, w których świadomość ochrony danych osobowych i przestrzegania przepisów jest niska, najczęściej najpierw powstaje proces, a potencjalne skutki jak i zasadność działań jest ustalana na późniejszych etapach, najczęściej w momencie wystąpienia skutków niepożądanych. Spółki, w których IOD w sposób prawidłowy realizuje swoje obowiązki i poszerza świadomość nie tylko pracowników, ale także kadry decyzyjnej, pojęcie "compliance" nabiera na znaczeniu. Spółki, które posiadają świadomość, jak istotne są działania projektowe przed wdrożeniem dane celu w życie, traktują *privacy by design* nie jako procedurę spowalniająca biznes, ale jako działanie zapewniające wysoką jakość usług, co z kolei pozwala uzyskać przewagę na rynku. Optymista stwierdzi, iż powodem do stosowania "privacy by design" jest budowanie przez IOD i rynek świadomości, jak istotna jest ochrona danych osobowych. Zdaniem pesymisty, stosowanie "privacy by design" jest skutkiem naruszenia dokonanego przez Administratora.

Należy mieć na uwadze, że nie każdy proces jest na tyle skomplikowany, aby niemożliwe było ustalenie celu w momencie rozpoczęcia działań. Każdy z nas działa w ramach utartych praktyk zawodowych. Wiemy, po co nam dane osobowe w preambule umowy, wiemy, dlaczego zbieramy dane kontaktowe naszego kontrahenta. Jeżeli przetwarzanie danych wynika z obowiązków nałożonych z mocy prawa, to co do zasady wiemy, dlaczego je zbieramy (chociaż nie zawsze jest to tożsame ze zrozumieniem powodów ustawodawcy). Problemy zaczynają się w chwili stosowania technologii - im nowsza, tym większe zamieszanie. Bardzo wiele przedsiębiorstw korzysta z systemu monitoringu, jednakże w jakim celu? Najczęściej przedsiębiorca informuje pracowników lub klientów, iż monitoring jest stosowany w celu zapewnienia bezpieczeństwa, jednakże w chwili wystąpienia czynu niepożądanego w obrębie monitoringu przedsiębiorcy bardzo usilnie bronią się przed oddaniem nagrania służbom lub osobie poszkodowanej. Monitoring bardzo "płynnie" zmienia swe cele – stosowany pierwotnie dla celów bezpieczeństwa potrafi np. w jednej chwili zacząć być przydatny w

celu ukarania pracownika, wskazując, iż celem monitoringu jest weryfikacja efektywności pracowników w miejscu pracy.

Brak zdefiniowania celu przetwarzania uwidocznił się w dobie pandemii koronawirusa. Mierzenie temperatury, kamery biometryczne, oświadczenie o nieprzebywaniu w krajach objętych pandemią - wszystkie te środki zaczęto rozważać lub stosować w spółkach w związku ze strachem przed COVID-19. Każde rozwiązanie można by uznać za uzasadnione, w celu potencjalnego wykrycia osoby zarażonej COVID-19, jednakże co się stanie w przypadku wykrycia takiej osoby? Czy poza stworzeniem procesu, ustalono jasny cel, a także ustalono, jakie mogą być skutki przetwarzania? Wielu przedsiębiorców, w szczególności z branży sprzedaży, nie potrafiło już odpowiedzieć na to pytanie, czy klient który posiada wyższą temperaturę zostanie wpuszczony na teren sklepu? A co, jeśli ma rękawiczki i maseczkę? Tworzenie procedur "na wypadek zdarzenia x" jest jak najbardziej dozwolone, np. backup, archiwizacja, plan zachowania ciągłości działania lub monitoring. Należy zawsze pamiętać, iż takie procedury powinny także uwzględniać, jak zadziałamy, jeżeli "zdarzenie x" faktycznie wystąpi.

Na gruncie RODO okazuje się, że nie tylko należy uważać, by w toku przetwarzania danych osobowych nie zgubić celu, lecz także by sam cel istniał. Przetwarzanie danych bez celu, może wiązać się ze znacznie groźniejszym skutkiem dla Spółki niż nagła zmiana celu - zmiana może być usprawiedliwiona, zaś brak celu już nie.

Damian Bielecki, Specjalista ds. ochrony danych osobowych iSecure Sp. z o.o.