RODO – PRZEKLEŃSTWO CZY BŁOGOSŁAWIEŃSTWO DLA BIZNESU?

Paweł BORKOWSKI
CEO,
Integral Solutions

W ostatnim czasie coraz więcej firm uświadamia sobie konieczność realizacji konkretnych działań w kontekście Rozporządzenia o Ochronie Danych Osobowych (RODO) znanego również jako GDPR. Rozporządzenie zostało wprowadzone w zeszłym roku przez Unię Europejską. Jest to o tyle ważna regulacja, że dotyczy wszystkich firm przetwarzających dane osobowe obywateli EU – w związku z tym podlegają jej również organizacje mające siedziby poza obszarem EU. Regulacja ta definiuje zakres danych osobowych, obowiązki firm względem osób prywatnych oraz ewentualne kary, które mogą być nałożone na firmę w przypadku stwierdzenia naruszeń.

Czy GDPR to coś więcej niż Data Governance?

Patrząc na zakres działań niezbędnych, aby dostosować się do tej regulacji, nasuwa się jednoznaczne skojarzenie z dobrymi praktykami dotyczącymi zarządzania danymi, które wprowadza się w ramach programów Data Governance. Jednakże uruchomienie takiego programu w organizacji wymaga zaangażowania zarządu, gdyż nie jest to inicjatywa, dla której możliwe jest łatwe obliczenie zwrotu z inwestycji. Dzisiaj firmy, które rozpoczęły już takie działania, albo są świadome wartości posiadanych zasobów, jakimi są dane, albo borykają się z dużymi problemami w zakresie prowadzenia zaawansowanych analiz pozwalających lepiej zrozumieć potrzeby klientów lub/i wyprzedzić konkurencję. Problemy te zazwyczaj wiążą sią z ograniczoną wiedzą o posiadanych danych w ramach całej organizacji, źródłach ich pochodzenia czy też ich znaczeniu. Wydaje się, że w wielu przypadkach regulacja GDPR poprawi świadomość organizacji w obszarze zarządzania danymi, co może przełożyć się na konkretne efekty biznesowe w zakresie lepszego wnioskowania na podstawie przeprowadzonych analiz, czy też optymalizacji przepływu informacji w kontekście procesów biznesowych. W niedługiej perspektywie może okazać się, że organizacja skorzysta na dostosowaniu się do GDPR.

Jak rozpocząć wprowadzanie zmian w organizacji w zakresie RODO w 12 krokach

Proponowane przez nas podejście do regulacji RODO bazuje na dwóch założeniach:

- Kluczowa jest wiedza o danych
- Należy dostosować rozwiązania do ryzyka związanego z danymi.

Te dwa założenia biorą się stąd, że ostatecznie większość działań skupia się na danych klientów.
Bazując na dwunastu krokach zaproponowanych przez Information Commissioner's Office (ICO) – odpowiednika naszego GIODO w Wielkiej Brytanii – proponujemy praktyczne podejście do znaczącego obniżenia ryzyka zapłacenia kar wynikających z regulacji.

Pierwszy krok to ŚWIADOMOŚĆ – czyli uzmysłowienie organizacji, czym jest regulacja i jakie wiążą się z nią zadania i ryzyka. W zależności od wielkości organizacji oraz jej złożoności konieczność zbudowania świadomości w tym zakresie może dotyczyć wyłącznie zarządu lub zarządu i departamentów zajmujących się takimi aspektami organizacji, jak bezpieczeństwo, compliance, kwestie prawne itp.
Trzeba również zapewnić platformę współpracy oraz wymiany informacji pomiędzy zarządem a osobami odpowiedzialnymi za dane lub procesy. Platforma ta powinna pomóc w uspójnieniu terminologii oraz prezentować informację właściwą dla każdej roli w procesie zarządzania danymi.

Drugi krok to POSIADANA INFORMACJA – czyli określenie, jakimi danymi osobowymi organizacja dysponuje, gdzie dokładnie się one znajdują, skąd pochodzą, jak przepływają poprzez systemy oraz gdzie ewentualnie opuszczają systemy. W ramach inwentaryzacji danych osobowych w pierwszym rzędzie należy zweryfikować, w jakich systemach oraz których tabelach tych systemów znajdują się dane wrażliwe. Dobrym posunięciem jest oczywiście zapoznanie się z dokumentacją systemu, aczkolwiek w wielu przypadkach może się to okazać niewystarczające. Dodatkowo zdarza się, że użyt-

kownicy systemów wpisują różne informacje w polach niekoniecznie przeznaczonych do przechowywania tego typu informacji (dzieje się to zwłaszcza w starszych tzw. pudełkowych rozwiązaniach). W takim przypadku ułatwieniem może być skorzystanie z usługi profilowania danych, która pomoże wskazać wszystkie miejsca zawierające dane osobowe zarówno w bazach danych, jak i w plikach niestrukturalnych (np. Excel, Word, PDF itp.).
Kolejnym działaniem jest utworzenie indeksu danych osobowych, który umożliwi sprawne wskazywanie miejsc przetwarzania takich danych w celu udostępnienia informacji o sposobie przetwarzania czy też w przypadku konieczności usunięcia danych lub ich przekazania nowemu podmiotowi. Taki indeks może być prostym spisem wystąpień danych osobowych lub też zaawansowanym rozwiązaniem typu „Customer 360", które jednocześnie może wspierać działania biznesowe – czyli przynosić dodatkowe wymierne korzyści.
Doświadczenie wskazuje, że jednym z największych wyzwań jest weryfikacja nieaktywnych systemów, dla których nie ma już dokumentacji, a pracownicy nie mają już wiedzy dotyczącej ich funkcjonowania. Jednym z sugerowanych rozwiązań jest utworzenie archiwum danych (w oparciu o dedykowane rozwiązanie), które umożliwi łatwe przechowywanie oraz przeszukiwanie nieaktywnych danych. Może być ono również zbawienne dla wszelkich „tasiemek" przechowywujących historyczne dane.

Trzeci krok to PRYWATNOŚĆ DANYCH – czyli weryfikacja klauzul, w ramach których osoba fizyczna wyraziła zgodę na przetwarzanie swoich danych osobowych. Ważną kwestią jest ustalenie, jakie klauzule są wymagane dla określonych procesów przetwarzania danych oraz przypisanie tych klauzul do właściwych systemów/procesów. Najlepszym rozwiązaniem byłoby powiązanie wspomnianych klauzul z indeksem/katalogiem procesów/systemów w organizacji.

Czwarty krok to PRAWA OSOBY – czyli możliwość zrealizowania prawa osób fizycznych do skasowania ich danych, tudzież ich udostępnienia w przyjaznym formacie. Idealnym rozwiązaniem wydaje się być przygotowanie szablonu procesu, który poprowadzi pracownika firmy przez niezbędne działania konieczne do przygotowania danych lub uruchomienia procesu kasowania danych.

Piąty krok to DOSTĘP DO DANYCH – czyli możliwość przedstawienia na żądanie danych osoby fizycznej wraz z opisaniem celu wykorzystania posiadanych danych. Analogicznie do punktu czwartego, wskazane byłoby posiadanie platformy, która przeprowadzi pracownika przez proces przygotowania informacji dla klienta. W platformie należałoby umieścić szablony dokumentów oraz opisy celów przetwarzania danych dla procesów/systemów wykorzystujących dane osobowe.

Szósty krok to PODSTAWY PRAWNE – czyli weryfikacja, czy wszystkie dane posiadane w organizacji pojawiły się w ramach kontrolowanych procesów i zostały pozyskane legalnie. Wskazane będzie udokumentowanie źródeł danych – szczególnie w przypadku pozyskiwania ich z zewnątrz organizacji.

Siódmy krok to ZGODY – czyli stworzenie spójnego katalogu zgód wyrażonych przez osoby fizyczne, dotyczące możliwości przetwarzania ich danych osobowych w kontekście procesów biznesowych. Dobrym rozwiązaniem byłoby połączenie katalogu zgód z katalogiem osób fizycznych utworzonym w kroku drugim. Jeszcze lepszą kontrolę nad stosowanymi zgodami uzyska się w sytuacji połączenia ich z katalogiem procesów, dla których takie zgody powinny zostać udzielone.

Ósmy krok to ZGODY WYRAŻONE W IMIENIU DZIECI – czyli dopilnowanie, aby, w przypadku przetwarzania danych dzieci poniżej 13 roku życia, zgodę na przetwarzanie wyrazili prawni opiekunowie dziecka. Sugerowane podejście jest analogiczne jak w poprzednim kroku.

Dziewiąty krok dotyczy WYCIEKU DANYCH. W związku z ryzykiem wycieku danych z systemów organizacji wymagane jest utworzenie sprawnego procesu informowania poszkodowanych o wycieku ich danych. W ramach platformy zarządzania procesami GDPR należałoby przewidzieć procesy, które byłyby pomocne w przypadku stwierdzenia wycieku danych, w oznaczeniu systemu, z którego taki wyciek nastąpił oraz ustaleniu skali wycieku. Przydatną informacją w takim przypadku będzie informacja opisująca, jakiego typu dane osobowe są przechowywane w systemie.

Dziesiąty krok polega na PROJEKTOWANIU OCHRONY – czyli usystematyzowanym podejściu do projektowania nowych systemów – „protection by design". W celu ułatwienia oraz usystematyzowania podejścia do projektowania własnych rozwiązań lub też w przypadku nabywania gotowych systemów sugerujemy utworzenie listy wymagań, jakie muszą zostać spełnione przez system dla danego obszaru danych, żeby można było uznać, że rozwiązanie zostało odpowiednio zaprojektowane. Umieszczenie takich wymagań w platformie zarządzania danymi sprawi, że w przypadku dołączania nowego systemu do architektury, po przypisaniu mu właściwych obszarów danych uzyskamy automatycznie listę wymagań do spełnienia przez taki system.

Jedenasty krok odnosi się do utworzenia roli CHIEF DATA OFFICER (lub podobnej) oraz wskazania osoby odpowiedzialnej za tę rolę w organizacji. Osoba taka powinna zostać wyposażona w odpowiednie instrumenty oraz umocowania w organizacji.

Ostatnim krokiem jest ustalenie JURYSDYKCJI, czyli zweryfikowanie lokalnych regulatorów zajmujących się regulacją GDPR w przypadku organizacji międzynarodowej. W takiej sytuacji istotne jest zdefiniowanie, która część organizacji jest administratorem danych, a która je tylko przetwarza.
Skuteczność przeprowadzonych w organizacji działań zmierzających do realizacji wymagań regulacji RODO wymaga również wdrożenia odpowiednich rozwiązań informatycznych.
Kompleksowe rozwiązania w zakresie zarządzania danymi od lat oferuje Informatica. Rozwiązania Informatica otrzymały od Gartnera najwyższe oceny aż w sześciu kluczowych obszarach zarządzania danymi.
Integral Solutions jako jedyny polski autoryzowany dystrybutor produktów Informatica serdecznie zaprasza organizacje i firmy do kontaktu, w celu przedstawienia oferty oraz konsultacji w zakresie wdrożenia regulacji RODO. ■

Integral Solutions
ul. Wspólna 35 lok. 1
00-519 Warszawa
tel.: +48 22 692 45 38