IBM

Droga do wygenerowania wartości

Tworzenie zrównoważonych, objętych kontrolą zasobów danych w związku z rozporządzeniem GDPR i innymi przepisami

IBM

1. GDPR jako szansa dla biznesu

Wprowadzenie ogólnego rozporządzenia o ochronie danych osobowych (General Data Protection Regulation – GDPR) i jego wejście w życie z dniem 25 maja 2018 r. stworzy nową równowagę między interesami przedsiębiorstw i prawami konsumentów w obszarze danych osobowych i danych wrażliwych. Każda osoba fizyczna udostępnia swoje dane osobowe przedsiębiorstwom – klienci robią to podczas transakcji, pracownicy w pracy, a partnerzy handlowi przy zawieraniu umów. Zamierzonym rezultatem wspomnianych przepisów są pozytywne i odpowiedzialne relacje z osobami, których dotyczą dane, oraz umożliwienie przedsiębiorstwom zrównoważonej działalności i nieprzerwanego tworzenia innowacji.

Jeszcze zanim to nowe środowisko stanie się rzeczywistością, prowadzone będą intensywne działania edukacyjne mające na celu zapoznanie osób fizycznych z ich nowymi prawami i przyczynami, dla których przedsiębiorstwa muszą przetwarzać ich dane. Obecnie świadomość w zakresie GDPR jest niska – tylko 10% ankietowanych konsumentów stwierdziło, że w pełni zdaje sobie sprawę z istnienia tego rozporządzenia (źródło: „GDPR Impact 2017", badanie z udziałem 1001 brytyjskich konsumentów, przeprowadzone przez firmę Research Now na zlecenie DataIQ, luty 2017 r.). Ochrona danych będzie jednak pewnego dnia powszechnie znanym zagadnieniem, podobnie jak to się już stało z kwestią ich zabezpieczeń. W czym tkwi różnica między ochroną i zabezpieczeniami? W przypadku ochrony danych chodzi o pokazanie plusów płynących z udostępniania danych, natomiast zabezpieczenia są często kojarzone z obroną przed minusami wynikającymi z naruszeń.

Czołowe przedsiębiorstwa działające w oparciu o dane pracują nad nowym podejściem do wymiany danych i ich wartości. Ma ono umożliwić osobom, których dotyczą dane, dostęp do danych i ich kontrolę, a zarazem wesprzeć podstawowe procesy biznesowe zrównoważonymi, nadzorowanymi przepływami danych. Rozporządzenie GDPR wymaga przeglądu całościowego przetwarzania danych, a rezultaty przeprowadzonych analiz powinny przynieść korzyści zarówno osobom, których dotyczą dane, jak i przedsiębiorstwom.

Wdrożenie tego pozytywnego podejścia może pomóc wygenerować wartość dla biznesu w dwóch wymiarach:

Wartość marki – gdy ludzie uświadomią sobie swoje nowe prawa, wybiorą te marki, które zapewnią im najszersze możliwości i najlepszą obsługę. Pozwoli to liderom zdobyć zaufanie i przewagę nad konkurencją.

Wartość biznesowa – dzięki usprawnieniu strategii w obszarze danych, wprowadzeniu wydajniejszego i lepiej zintegrowanego przetwarzania danych oraz dostosowaniu systemów operacyjnych do wymogów GDPR firmy mogą obniżyć koszty.

2. GDPR – budowanie na solidnych fundamentach

Rozporządzenie GDPR wejdzie w życie po 20 latach od wprowadzenia dotychczasowej unijnej dyrektywy o ochronie danych. Przez ten czas zmieniło się praktycznie wszystko – od typów generowanych danych przez procesy używane do ich rejestrowania i nadzorowania aż po systemy do ich analizowania i wykorzystywania oraz zarządzania nimi. Przedsiębiorstwa, które przestrzegają już podstawowych zasad wynikających z obowiązujących przepisów, są dobrze przygotowane na wdrożenie nowego rozporządzenia. Warto jednak pamiętać, że niezbędne rozszerzenia i udoskonalenia będą wymagać staranności.

Dane osobowe stały się bardziej osobiste Rozporządzenie GDPR rozszerza definicję danych osobowych na niemal wszystko, co może zidentyfikować osobę fizyczną, jak choćby jej lokalizację, używane przez nią treści lub aplikacje (dane dotyczące zachowań) oraz używane urządzenie (identyfikator urządzenia). Dane nieustrukturyzowane, takie jak komentarze klientów, recenzje, wpisy na blogach, notatki dotyczące obsługi klienta, wiadomości e-mail związane z zarządzaniem kontem, a nawet komunikaty wewnętrzne – to wszystko są informacje, które muszą zostać objęte nadzorem.

Większe możliwości w zakresie dostępu i zgód Oprócz istniejących praw, takich jak możliwość dostępu do danych i ich poprawienia, osoby fizyczne otrzymają rozszerzone prawa, w tym prawo do wycofania zgody, przeniesienia danych osobowych do innego dostawcy, a nawet zażądania usunięcia danych.

W Europie i na świecie Każda osoba z Unii Europejskiej, której dotyczą dane, może oczekiwać, że wspomniane wyżej prawa będą chronione niezależnie od miejsca przechowywania lub przetwarzania danych. Prawa te będą towarzyszyć danym również w przypadku ich przeniesienia poza UE, dlatego przenoszenie danych osobowych między regionami będzie wymagało ostrożności.

Całościowa odpowiedzialność Administratorzy danych będą musieli nie tylko dbać o przestrzeganie przepisów GDPR we własnych przedsiębiorstwach, lecz także upewnić się, że ich partnerzy handlowi (podmioty przetwarzające dane) również działają zgodnie z tym rozporządzeniem. Obie strony są odpowiedzialne za bezpieczeństwo danych, mają też nowe obowiązki związane z raportowaniem naruszeń w tym zakresie.

Nowe obowiązki w obszarze danych Rozporządzenie wprowadza szereg nowych wymagań, w szczególności konieczność powołania inspektora ochrony danych, a także wdrożenia nowych strategii nadzoru i rozwiązań opartych na ryzyku.

Większe możliwości egzekwowania Większe uprawnienia organów ochrony danych są kluczowe dla skutecznego wdrożenia przepisów GDPR. Instytucje te mogą w szczególności nakładać grzywny w wysokości sięgającej 4% rocznych globalnych obrotów grupy lub 20 mln EUR (w zależności od tego, która z tych kwot jest wyższa).

3. Najważniejsze kroki na drodze do wygenerowania wartości

Zamiarem przyświecającym twórcom GDPR jest wypracowanie lepszej równowagi między zgodnymi z prawem interesami firm a prawami osób, których dotyczą dane. Aby sprostać wymogom rozporządzenia i wydobyć nową wartość ze zrównoważonych, objętych kontrolą zasobów danych, niezbędne jest kreatywne, przezroczyste i praktyczne rozwiązanie.

IBM zidentyfikował pięć ważnych kroków, które powinny zostać uwzględnione przez przedsiębiorstwa:

Nadzór nad realizacją – kluczowym elementem GDPR jest zaangażowanie wszystkich działów przedsiębiorstwa w odpowiedni sposób rejestrowania, przetwarzania, ochrony i wykorzystywania danych osobowych oraz zarządzania nimi. Rozpoczyna się to na poziomie strategicznym od wdrożenia zasady uwzględniania ochrony prywatności już w fazie projektowania nowych procesów uzależnionych od danych, połączonej z oceną skutków przetwarzania dla ochrony danych. Pozwala to określać czynniki ryzyka i zagrożenia dla wszelkich elementów danych wrażliwych.

Zrozumiałe i przejrzyste wyjaśnienie osobom fizycznym, dlaczego ich dane są potrzebne oraz w jaki sposób i jak długo będą wykorzystywane i zarządzane, będzie wymagać modyfikacji oświadczeń o ochronie prywatności. Poszczególne zgody i sformułowania należy rejestrować dla każdego rekordu. Nadzór nad tą kwestią w całym przedsiębiorstwie będzie obowiązkiem inspektora ochrony danych, mającego konkretne obowiązki, status i wsparcie. Stanowisko to może po dodatkowych szkoleniach objąć osoba wykonująca dotychczas zbliżone zadania, jednak może się okazać konieczne zatrudnienie nowego pracownika. Tańszą alternatywą jest skorzystanie ze wspólnego inspektora ochrony danych w ramach outsourcingu.

Nadzorem tym mogą zostać objęte osoby trzecie, takie jak podmioty przetwarzające dane na kolejnych etapach. Firma powinna sprawdzić, czy tacy partnerzy handlowi przestrzegają rozporządzenia GDPR, oraz szczegółowo opisać tę kwestię we wszelkich porozumieniach umownych.

Prawa i procesy – osoby, których dotyczą dane, otrzymują dodatkowe prawa – np. możliwość wycofania zgody oraz przeniesienia i usunięcia danych – rozszerzające ich dotychczasowe uprawnienia, takie jak możliwość poprawienia danych i złożenia wniosku o ich udostępnienie. Zaspokojenie potrzeb wynikających z tych praw może wymagać rozległych prac programistycznych. Kluczową rolę odegrają tu rozwiązania techniczne i zrewidowane strategie.

Dostosowania do rozporządzenia GDPR mogą również wymagać procesy biznesowe. Trzeba będzie przeanalizować i w razie potrzeby zmodyfikować funkcje frontowe, takie jak zarządzanie relacjami z klientami, które są w bardzo dużej mierze uzależnione od danych osobowych. Zmiany będą też konieczne w funkcjach zaplecza, np. w systemach kadrowych, tak aby pracownicy mogli korzystać ze swoich praw, a firma uniknęła ryzyka wynikającego z przetwarzania danych osobowych nieobjętych nadzorem.

Dane – dane napływają do przedsiębiorstwa ze wszystkich procesów i kanałów biznesowych, a także z zewnątrz, za pośrednictwem marketingu cyfrowego, partnerów dystrybucyjnych i innych punktów kontaktu. Jeśli model biznesowy firmy zasadniczo opiera się na takim przepływie danych osobowych, to niezbędny jest program badania i kontroli danych. Odwzorowanie typów wykorzystywanych danych i miejsca ich przechowywania oraz określenie, czy są to dane wrażliwe, pozwoli stworzyć środowisko, w którym musi się poruszać przedsiębiorstwo w celu spełnienia wymogów GDPR.

Kluczowa będzie tu integracja wszystkich tych zestawów danych w celu uzyskania pełnego obrazu – stworzenie widoku poszczególnych klientów pozwoli zapewnić osobom fizycznym dostęp, kontrolę i możliwość poprawiania lub wyodrębniania własnych danych osobowych zgodnie z przepisami, a zarazem stanie się podstawą dla przyszłego generowania wartości z przepływu danych. Pomoże to również zadbać o odpowiednie zarządzanie cyklem życia informacji, w tym – w razie potrzeby i zgodnie z prawem – usuwanie rekordów klientów.

Bezpieczeństwo danych – zapewnienie bezpieczeństwa danych osobowych jest kluczowym elementem wymaganej ochrony danych. Zabezpieczenia danych powinny nie tylko chronić cenne zasoby biznesowe, lecz także być elementem obietnicy składanej klientom, którzy coraz częściej obawiają się zagrożeń wynikających z naruszeń ochrony i utraty ich danych. W epoce relacji opartych na zaufaniu, która ma nastąpić po wdrożeniu rozporządzenia GDPR, inwestycja w odpowiednie zabezpieczenia danych może być elementem wyróżniającym firmę na tle konkurencji.

Jednym z najtrudniejszych do spełnienia wymogów GDPR będzie prawdopodobnie konieczność informowania regulatora o każdym naruszeniu ochrony danych w ciągu 72 godzin od jego wykrycia oraz powiadamiania o tym osób fizycznych dotkniętych naruszeniem w stosownym terminie. Wdrożenie zgodnych ze standardem branżowym narzędzi do zarządzania dostępem do danych i monitorowania zabezpieczeń oraz lepsza koordynacja reagowania na incydenty mogą przygotować firmę na spełnienie tego rygorystycznego obowiązku.

Ludzie i komunikacja – ludzki wymiar dostosowywania przedsiębiorstw do rozporządzenia GDPR wymaga połączenia komunikacji formalnej i ciągłego uwrażliwiania personelu na tę kwestię. Wiadomości dostosowane do poszczególnych ról i zbiorcza komunikacja korporacyjna powinny informować o nowych procedurach roboczych i pokazywać nową kulturę przedsiębiorstwa.

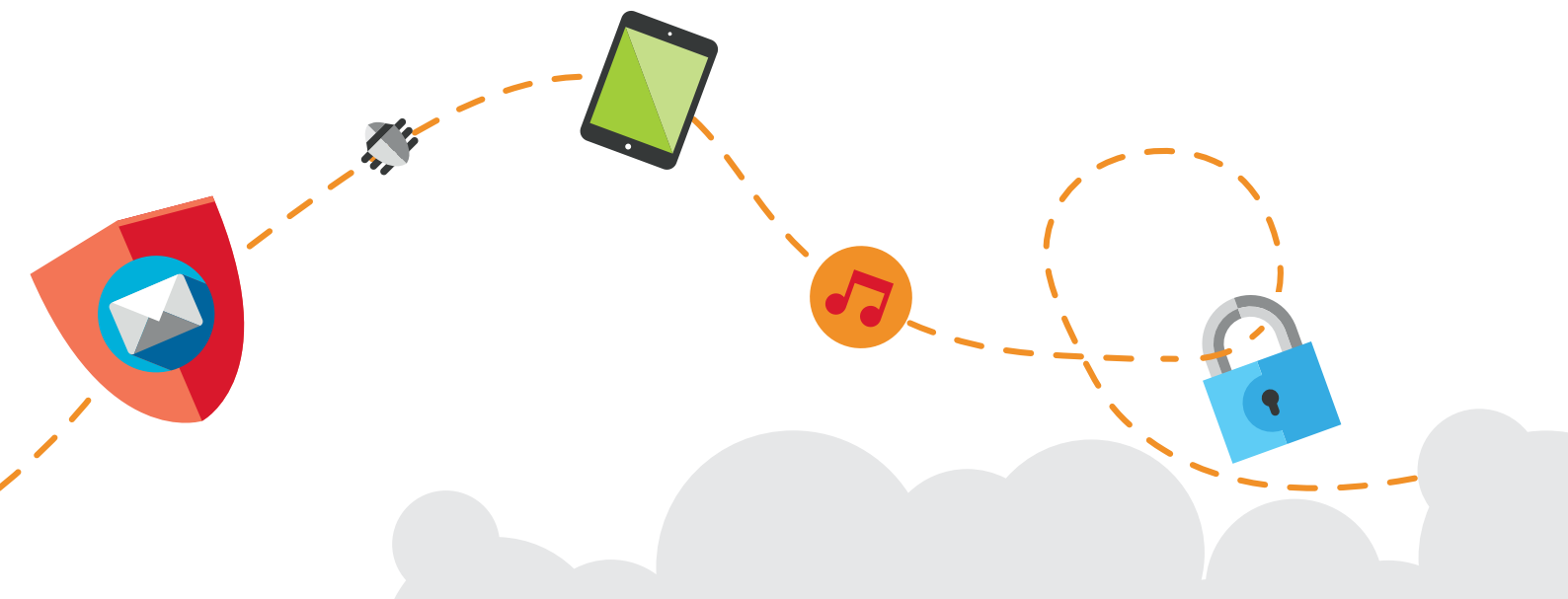
Budowanie personelu, który rozumie konieczność traktowania danych osobowych jako istotnych zasobów biznesowych i zdaje sobie sprawę z obowiązku szanowania praw osób fizycznych w zakresie dotyczących ich danych, może wymagać szeroko zakrojonych szkoleń wstępnych i ich regularnego odświeżania. W program wdrażania GDPR należy więc włączyć dobrze ustrukturyzowane programy szkoleniowe, w szczególności realizowane jako usługa.

4. IBM jako przewodnik dla firm

IBM dysponuje kompleksowym rozwiązaniem, dzięki któremu jest w stanie wspierać przedsiębiorstwa w realizacji programów przygotowujących je na wdrożenie rozporządzenia GDPR. Nasze kwalifikacje w obszarze globalnych usług biznesowych, prawnie zastrzeżone technologie i innowacje związane z zarządzaniem ochroną prywatności sprawiają, że możemy pomóc firmom w tych przygotowaniach.

Warto dodać, że my również podążamy tą drogą. IBM realizuje własny projekt GDPR, możemy więc wymieniać się wnioskami wyciągniętymi z własnych doświadczeń, a także dzielić się skutecznymi rozwiązaniami, poznanymi dzięki asystowaniu naszym Klientom.

- **Doświadczeni konsultanci** – eksperci w swoich dziedzinach, dogłębnie znający zagadnienie ochrony danych.
- **Zarządzanie zmianami biznesowymi** – kapitał intelektualny, zasoby i narzędzia pomagające w transformacji procesów biznesowych.
- **Rozwiązania technologiczne** – od zarządzania danymi i zarządzania cyklem życia informacji po bezpieczeństwo informacji i raportowanie incydentów.
- **Całościowa oferta** – ścisła koncentracja na newralgicznych zmianach, które należy wprowadzić do 25 maja 2018 r., a także na długoterminowym generowaniu wartości.



Więcej informacji

Aby uzyskać więcej informacji o rozporządzeniu GDPR i rozwiązaniach IBM, które pomagają firmom w ochronie i poznawaniu ich danych oraz zarządzaniu nimi, należy skontaktować się z przedstawicielem IBM lub odwiedzić serwis WWW:

ibm.com/gdpr

IBM Polska Sp. z o.o.
ul. Krakowiaków 32
02-255 Warszawa

Strona główna IBM znajduje się pod adresem:
ibm.com

Zawarte w niniejszym dokumencie odwołania do produktów i usług IBM nie oznaczają, że IBM zamierza udostępnić je we wszystkich krajach, w których prowadzi działalność.

Uwaga: za przestrzeganie we własnym przedsiębiorstwie stosownych praw i przepisów, w tym rozporządzenia GDPR, odpowiada Klient. Klient ponosi wyłączną odpowiedzialność za uzyskanie porady kompetentnego radcy prawnego w kwestii ustalenia i interpretowania przepisów prawnych i regulacji mających związek z działalnością Klienta oraz za podjęcie odpowiednich czynności w celu zapewnienia ich przestrzegania. Produkty, usługi i inne możliwości opisane w niniejszym dokumencie nie muszą odpowiadać sytuacji wszystkich Klientów, a ich dostępność może być ograniczona. IBM nie udziela porad w zakresie prawa, księgowości ani audytu, a także nie oświadcza i nie gwarantuje, że usługi lub produkty IBM zapewnią przestrzeganie prawa przez Klienta.

Odzyskuj surowce wtórne