Dawid Wiśniewski

Po co to RODO i czy trzeba się go bać?

Why do we need GDRP and should we fear it?

Słowa kluczowe:
RODO, IOD, Prezes Urzędu Ochrony Danych Osobowych, administrator

Dawid Wiśniewski
Specjalista ds. ochrony danych osobowych
tel. 885 750 184
dawid.wisniewski@mbmtychy.pl
MBM TYCHY
ul. Metalowa 3, 43-100 Tychy

Chyba nie ma osoby, która w ostatnich miesiącach nie słyszałaby o RODO. Niemal każdego dnia przedsiębiorcy byli (i nadal są) zasypywani licznymi propozycjami wdrożenia odpowiednich środków mających zapewnić bezpieczeństwo przetwarzanym przez nich danym osobowych pracowników czy klientów. Niestety świadomość obowiązków, jakie ciążą na właścicielach firm nadal pozostawia wiele do życzenia, podczas gdy znajomość praw wśród osób, których dane są przetwarzane stale rośnie. Niniejszy artykuł ma za zadanie pokazać, że nie taki diabeł straszny jak go malują, a zastosowanie kilku, często gotowych rozwiązań, może pomóc ustrzec się przed przykrymi konsekwencjami niedostosowania się do RODO.

RODO, czyli ujednolicenie przepisów

RODO, czyli ogólne rozporządzenie o ochronie danych osobowych z 27 kwietnia 2016 r. wprowadza w tym temacie reguły takie same dla wszystkich w całej Unii Europejskiej. Do stosowania zasad zgodnych z RODO zobowiązane są także te podmioty, które

Streszczenie

Chyba nie ma osoby, która w ostatnich miesiącach nie słyszałaby o RODO. Niemal każdego dnia przedsiębiorcy byli (i nadal są) zasypywani licznymi propozycjami wdrożenia odpowiednich środków mających zapewnić bezpieczeństwo przetwarzanym przez nich danym osobowych pracowników czy klientów. Niestety świadomość obowiązków jakie ciążą na właścicielach firm nadal pozostawia wiele do życzenia, podczas gdy znajomość praw wśród osób, których dane są przetwarzane stale rośnie. Niniejszy artykuł ma za zadanie pokazać, że nie taki diabeł straszny jak go malują, a zastosowanie kilku, często gotowych rozwiązań, może pomóc ustrzec się przed przykrymi konsekwencjami niedostosowania się do RODO.

Abstract

There are probably very few people who in the recent months have not heard about GDRP (General Data Protection Regulation). Business owners were (and still are) being inundated with multiple offers of implementing the necessary mechanisms of protecting their customers' personal data which they are processing. Unfortunately, the overall awareness of the obligations which have been bestowed upon business owners leaves a lot to be desired, while the knowledge of the introduced laws among those whose data are being processed is constantly increasing. This article will show that GDRP should not make our blood run cold and that using a few, often ready-made, solutions can help you protect your business from the consequences of not adhering to GDRP regulations.

są poza UE, ale korzystają z danych jej obywateli. Głównym założeniem RODO miało być ujednolicenie oraz ucywilizowanie zasad przetwarzania danych.

Niniejsze rozporządzenie nie wprowadza żadnych rewolucyjnych zmian w podejściu do ochrony danych osobowych. I choć administrator danych osobowych (dawniej ADO) zmienia się w administratora, w miejsce Administratora bezpieczeństwa informacji (ABI) pojawia się Inspektor ochrony danych (IOD), nie ma konieczności prowadzenia w dotychczasowej formie Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym i nie musimy już zgłaszać zbiorów danych do GIODO to założenie nadal jest takie samo jak przy ustawie o ochronie danych osobowych z 1997 r. – pozyskiwać z legalnych źródeł dane osobowe i odpowiednio je zabezpieczać przed utratą, zniszczeniem czy nieuprawnionym dostępem.

RODO to akt prawny, który w swoim założeniu nie daje administratorowi gotowej listy dokumentów lub zabezpieczeń, pozostawiając nieco swobody w kwestii wdrożenia odpowiednich środków, dzięki którym będzie można wykazać stosowanie przepisów o ochronie danych osobowych. Podczas opracowywania unijnego rozporządzenia wielokrotnie podkreślano, że ma być to rozporządzenie uniwersalne, takie, którego zapisy nie stracą na ważności za 10 czy 20 lat. Tak też można wytłumaczyć, w odróżnieniu od dotychczasowych przepisów, które nas obowiązywały, dlaczego nie ma kompletnej listy dokumentów, które należy zastosować w podmiocie. Każdy administrator musi sam dokonać analizy środków technicznych i organizacyjnych, jakie stosuje podczas przetwarzania danych osobowych. Wszystkie rozwiązania muszą być indywidualnie dostosowane do rodzaju prowadzonej działalności, wielkości podmiotu oraz działań, jakie administrator wykonuje na danych osobowych.

Obowiązki administratora zgodnie z RODO

Jeżeli chodzi o obowiązek prowadzenia dokumentacji, to w RODO można znaleźć informację, że należy prowadzić „rejestr czynności przetwarzania" między innymi w zakresie przetwarzania danych szczególnej kategorii (np. danych o stanie zdrowia, genetycznych) oraz dla wszelkich czynności na danych osobowych, które nie mają charakteru sporadycznego (np. dotyczących obsługi kadrowo-płacowej pracowników). Jak się okazuje nieco kłopotu przysparza identyfikacja poszczególnych czynności, lecz z pomocą specjalistów i przy odrobinie chęci temat można całkiem sprawnie zorganizować.

W związku z tym, że każdy właściciel firmy ma wiele innych, na pewno ważniejszych zadań do wykonania, RODO często staje się kolejnym i niestety przykrym obowiązkiem, który narzuca UE.

Dlatego, aby nie narażać się na niechciane kontrole, oskarżenia klientów i pracowników o niestosowanie właściwych przepisów dotyczących przetwarzania danych osobowych, tak ważne jest, aby administrator poznał swoje podstawowe obowiązki oraz miał wiedzę jak zastosować je w praktyce.

Jednym z nowych obowiązków, na który kładzie się szczególny nacisk i wokół którego jest najwięcej zamieszania, jest obowiązek informacyjny wobec osób, których dane się przetwarza. Bez wątpienia można powiedzieć, że klauzule informacyjne sprawiają sporo trudności, nie tylko administratorom, ale bardzo często również Inspektorom ochrony danych – teoretycznie przygotowującym się od 2 lat do pełnienia tej funkcji. Administrator musi, zgodnie ze ścisłym instrukcjami wynikającymi z RODO, poinformować każdą osobę m.in. o tym jakie jej dane posiada, w jakim celu je przetwarza, jakie prawa przysługują tej osobie.

Jeżeli mowa już o prawach, jakie przysługują osobom podającym dane osobowe, to RODO wprowadza kilka zasad, które do tej pory nie funkcjonowały w polskim prawie: prawo do bycia zapomnianym, prawo żądania usunięcia danych, prawo do sprzeciwu, prawo do ograniczenia przetwarzania, prawo do przenoszenia danych. I choć bez wątpienia są to prawa tych osób, to dla administratorów często stają się one po prostu kolejnymi obowiązkami, z których musi on zdawać sobie sprawę i w odpowiedni sposób reagować na różnego rodzaju wnioski płynące ze strony pracowników czy klientów.

Kwestia pracowników, nadanie im upoważnień do przetwarzania danych osobowych zgodnych z RODO oraz zapewnienia im odpowiedniej wiedzy z zakresu ochrony danych osobowych to już zupełnie inny temat. Niestety, jak w wielu innych przypadkach, to czynnik ludzki staje się największym zagrożeniem w trakcie pracy. Oczywiście zakładamy, że nikt specjalnie nie będzie udostępniał danych Państwa pacjentów, ale tylko odpowiednie przeszkolenie personelu ochroni administratora przed przykrymi konsekwencjami i roszczeniami ze strony klientów. Dobrą praktyką administratorów, zalecaną jeszcze przez GIODO (Generalnego Inspektora Ochrony Danych Osobowych – dotychczasowy organ nadzorczy zastąpiony przez Prezesa Urzędu Ochrony Danych Osobowych) jest organizowanie cyklicznych szkoleń dla pracowników. Co do zasady - szkolenie powinna przejść każda osoba dopuszczona

do przetwarzania danych osobowych. W ostatnim czasie często słyszy się o różnych ofertach szkoleniowych i choć Prezes Urzędu Ochrony Danych Osobowych dopuszcza korzystanie z doradztwa innych podmiotów, to mocno uczula administratorów na baczne przyglądanie się ich referencjom.

IOD – wsparcie?

Jak widać z powyższej części artykułu, ilość zadań i rozwiązań, które musi wprowadzić administrator jest znacząca. Nie da się ukryć, że to tylko ułamek tego co każdy przedsiębiorca musi robić, aby działać zgodnie z prawem. W kwestiach RODO pomocne może okazać się wsparcie Inspektora ochrony danych wśród obowiązków którego znajduje się m.in. „informowanie administratora, (…) pracowników o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia", „monitorowanie przestrzegania niniejszego rozporządzenia". Każdy administrator musi przeanalizować czy zgodnie z art. 37 RODO spoczywa na nim obowiązek wyznaczenia Inspektora, a jeżeli po analizie okaże się, że nie, to biorąc pod uwagę specyfikę swojej działalności może taką osobę u siebie wyznaczyć.

Jeżeli chodzi o branżę medyczną to należy zwrócić szczególną uwagę na zapisy art. 37 pkt 1c, który mówi, że obowiązek wyznaczenia IOD ma podmiot wtedy, gdy „główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10". Nie można zapominać, że mimo iż powołanie IOD to w niektórych przypadkach obowiązek, a czasem dobrowolna decyzja, to i tak pełną odpowiedzialność za wdrożenie odpowiednich środków technicznych i organizacyjnych ponosi administrator. I tutaj kwestia konieczności posiadanie odpowiedniej wiedzy zatacza krąg: bo jak administrator ma wiedzieć czy IOD prawidłowo mu doradza i wprowadza system ochrony danych? Dlatego też apelujemy w tym miejscu do administratorów, aby rozważnie wybierali osobę do pełnienia funkcji IOD tzn. sprawdzili jej wiedzę, nie tylko z zakresu RODO, ale również ze znajomości przepisów branżowych, poprosili o odpowiednie potwierdzenie jego umiejętności, a jeszcze lepiej o jego referencje. Tylko wybór odpowiedniej osoby i umiejętność sprawdzenia jej wiedzy daje gwarancję, że administrator może siebie odciążyć w tym temacie.

Odpowiedzialność administratora

Założeniem tego artykułu nie jest strasznie karami, ale warto wspomnieć, co grozi za nieprzestrzeganie nowych przepisów. Jak wynika z ankiety przeprowadzonej przez GIODO na początku roku największa świadomość przedsiębiorców jest właśnie w zakresie wysokości kar przewidzianych zapisami RODO. Zgodnie z art. 83 pkt 9 RODO „nakładane kary pieniężne muszą być w każdym przypadku skuteczne, proporcjonalne i odstraszające", aby przyniosły pożądany efekt i zapobiegły podobnym sytuacjom.

Wracając do tematu wysokiej świadomości obywateli, należy podkreślić, że RODO daje osobom, których dane są przetwarzane nowe narzędzie – możliwość wniesienia skargi do organu nadzorczego i ubieganie się o odszkodowanie od administratora. W opinii ekspertów ten zapis niniejszego rozporządzenia staje się najbardziej niebezpieczny, ponieważ mimo najlepszych chęci administratora, nie ma on pełnego wpływu na działania osób sobie podległych.

W kontekście odpowiedzialności, jaka ciąży na administratorze ważną kwestią jest również nadzór nad przypadkami uchybień i zagrożeń, a tym samym ich identyfikacja, skuteczne ich monitorowanie, analizowanie i zapobieganie kolejnym zdarzeniom zagrażającym bezpieczeństwu danych.

Podsumowanie

Pozostając w kręgu medycznym można powiedzieć, że lepiej zapobiegać niż leczyć. Najważniejsze zatem jest, aby każdy mający dostęp do danych tj. administrator, osoba upoważniona do przetwarzania danych miał świadomość, że RODO powstało w celu wprowadzenia normalności w pozyskiwaniu i przetwarzaniu danych. Plan wydaje się prosty i tak naprawdę zamknie się w 3 etapach: zaplanować, wdrożyć i stosować system prawidłowego przetwarzania danych osobowych. Jeżeli dodać do tego szereg gotowych rozwiązań, które proponuje rynek, to cały proces nie wydaje się już taki straszny, jak na samym początku.

Do organizacji prawidłowej ochrony danych osobowych należy więc podejść spokojnie, bez paniki i przede wszystkim ze zdrowym rozsądkiem. Ważne by umieć udowodnić, że administrator realizuje swoje obowiązki zgodnie z ogólnymi wytycznymi z uwzględnieniem ryzyka naruszenia praw lub wolności osób fizycznych, swojej najlepszej wiedzy i swoich możliwości. Należy wykazać zarówno organowi nadzorczemu, jak i osobom, których dane się przetwarza, że dbamy o ochronę danych osobowych i że osoby te mogą się czuć bezpieczne korzystając z usług podmiotu, dla którego temat RODO jest ważny.

Piśmiennictwo

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000),

[3] https://uodo.gov.pl/