Zeszyty Naukowe Gdańskiej Szkoły Wyższej
ISSN 2300-9055 2018, Nr 2(19), s. 229–232
Kwartalnik DOI 10.24426/zngsw.v19i2.41

Martyna Bubiłek
studentka, Gdańska Szkoła Wyższa

Wejście w życie Rozporządzenia Ogólnego Danych Osobowych

Streszczenie
Rozporządzenie Ogólne Danych Osobowych, jako zwrot ostatnio dosyć popularny, wywołuje najczęściej negatywne emocje. Nie raz słychać było wiele niepochlebnych opinii na ten temat, przez co niechętnie do niego podchodzimy. Artykuł umożliwia spojrzenie na RODO z innej perspektywy: jaki nacisk kładziony jest na ochronę naszych danych osobowych oraz z czym wiąże się nieprzestrzeganie tych zasad.

Słowa kluczowe: RODO, bezpieczeństwo, dane, ochrona, zabezpieczenie.

Z pewnością każdy słyszał o Rozporządzeniu Ogólnym Danych Osobowych — RODO (*Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*), które wprowadziło spory chaos wokół nas. Zdania na temat RODO są bardzo podzielone: jedni są jego zwolennikami inni, przeciwnie, uważają Rozporządzenie za bardzo nietrafiony pomysł, który tylko utrudnia życie. Skąd takie przekonanie? Być może z powodu niedoinformowania, a być może przez media, które kreują obraz RODO jako coś, czego powinniśmy się bać. Ludzie boją się zmian, nie wiedzą, czego można się spodziewać. Jednak gdy zapoznają się z tym lepiej, często okazuje się, że nie taki diabeł straszny, jak go malują i właśnie tą tezę chciałabym udowodnić w mojej publikacji.

Projekt Rozporządzenia Ogólnego Danych Osobowych opracowywano przez 4 lata, ostatecznie został przyjęty przez Parlament Europejski i Radę Europejską i obowiązuje od 25 maja 2018 r.

Rewolucja, której jesteśmy świadkami, następuje po ponad 20 latach od uchwalenia Dyrektywy o ochronie danych osobowych, będącej „matką" obecnych przepisów w całej Unii Europejskiej (*Kompendium wiedzy na temat RODO*). Dyrektywa ta ustala zasady zbierania, gromadzenia, przechowywania i udostępniania danych osobowych oraz określa warunki zgodności ich przetwarzania z prawem, a także zawiera prawa osób, których te dane dotyczą. Mimo tej ustawy ilość zorientowanych i stosujących się do tego Polaków jest bardzo mała.

Na czym polega to rozporządzenie? Otóż od dnia 25 maja 2018 r. wszelkie dane osobowe znajdujące się w przeróżnych bazach danych, serwerach, w poczcie internetowej, czy nawet na dyskach i urządzeniach mobilnych, będą pod ścisłą kontrolą. Dotyczy to naszych pracodawców, Policji i innych służb publicznych, a nawet nas samych.

RODO wprowadza dwie nowe zasady:

1. *Privacy by design* (prywatność projektu) — obowiązek administratora danych do uwzględniania zagadnień prywatności już na etapie opracowania sposobów przetwarzania danych, jak również na każdym etapie faktycznego przetwarzania. Oznacza to, że dane muszą być rozliczane, bezpiecznie przechowywane i udostępniane tylko osobom do tego uprawnionym.
2. *Privacy by default* (prywatność domyślna) — zobowiązanie administratorów danych do wdrożenia i stosowania takich środków zarówno technicznych, jak również organizacyjnych, które zapewnią przetwarzanie tylko danych koniecznych w celu ich przetwarzania.

Służby publiczne, którym niezbędne jest udostępnianie danych osobowych, mają prawo żądać niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej. Wymienione podmioty w zakresie swojego działania zobligowane są do udzielenia tej pomocy.

Zgodnie z art. 14 ust. 4 *ustawy z dnia 6 kwietnia 1990 r. o Policji*, służba ta bez wiedzy i zgody osoby, której te dane dotyczą, może żądać udostępnienia dokumentacji ochrony danych osobowych nawet, jeśli jest ona określona jako tajna. Oznacza to, że Policja jest jedną z niewielu jednostek, które są wyłączone z ustawy. Jeśli dokumentacja nie jest oznaczona jako tajna, ale załączniki do niej już są zastrzeżone, administrator danych nie może odmówić Policji udostępnienia takiej dokumentacji wraz z załącznikami. Według prawa jest wręcz zobowiązany przekazać całą dokumentację. Aby otrzymać taką dokumentację, mundurowi muszą wystąpić pisemnie z prośbą; powinna być ona uzasadniona, mieć charakter wyjątkowy oraz nie powinna dotyczyć całego zbioru danych osobowych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, służby powinny robić to zgodnie z celem przetwarzania.

Natomiast inaczej jest w przypadku, gdy potrzebne są informacje oznaczone jako niejawne. W takiej sytuacji udostępnianie danych musi odbywać się zgodnie z zasadami określonymi w ustawie o ochronie informacji niejawnych oraz aktach wykonawczych do tej ustawy. Zabrania się więc udostępniania dokumentacji ochrony danych osobowych funkcjonariuszowi, który nie spełnia wymogów opisanych w ustawie.

Zgodę na pozyskiwanie danych osobowych regulują takie akty prawne, jak: Kodeks karny, Kodeks wykroczeń, Kodeks postępowania karnego, Kodeks postępowania w sprawach wykroczeń.

Osoba, której te dane dotyczą, zgodnie z art. 32 ust. 1 *ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* ma prawo do uzyskania następujących informacji:

– istnieniu takiego zbioru oraz o ustaleniu administratora danych, adresu jego siedziby i pełnej nazwy,

– celu, zakresie i sposobie przetwarzania danych,
– źródle, z którego pochodzą dane jej dotyczące,
– sposobie udostępniania danych i o odbiorcach tych danych.

Może również żądać sprostowania, uaktualnienia, a nawet wstrzymania przetwarzania danych, jeśli są one niekompletne, nieprawdziwe, czy po prostu zbędne (*Podstawowe zagadnienia dotyczące ochrony danych osobowych (z testem)*, 2014).

Artykuł 9 *ustawy z dnia 10 czerwca 2016 r. o działaniu antyterrorystycznym* mówi, iż: *w celu zapobiegania lub zwalczania przestępstw o charakterze antyterrorystycznym Szef ABW może zarządzić niejawne prowadzenie czynności polegających na* (…) *wyszukiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej a pomocą środków komunikacji elektronicznej, a także uzyskiwaniu i utrwalaniu danych zawartych na informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych*. Z ustawy wynika, że w tym wypadku również występuje ochrona danych osobowych nie tylko obywateli naszego kraju, ale również obcokrajowców, a do nich mają dostęp tylko uprawnione do tego służby.

Jednak mimo tego, że nasze dane osobowe są chronione, niestety często zdarzają się wycieki przez podstawowe błędy, które nie powinny mieć miejsca. Do najczęściej popełnianych błędów związanych z naruszeniem danych osobowych należą (Skelnik, 2018):

– brak szyfrowania przesyłanych danych,
– masowa wysyłka maili z otwartą listą mailingową,
– zapisywanie danych na dyskach bez ich szyfrowania,
– zatrudnianie na tak odpowiedzialnych stanowiskach niewykwalifikowanych pracowników, którzy mają bezpośredni wpływ na bezpieczeństwo danych osobowych.

Przez takie błędy nasze dane mogą wpaść w niepowołane ręce i mogą zostać wykorzystane oczywiście na naszą niekorzyść. Dlatego za dopuszczenie się takiego czynu RODO wprowadza kary finansowe nawet do 20 mln euro. Nie bójmy się więc zgłaszać naszych wątpliwości co do przechowywania naszych danych. Mamy prawo poinformować o tym Generalnego Inspektora Ochrony Danych Osobowych, który z pewnością nam pomoże rozwiązać problem. Za umyślne popełnienie takiego czynu grożą kary w postaci odszkodowania, wpłaty na cel społeczny, przeprosin oraz podjęcia działań mających na celu likwidację jego skutków, a nawet do 2 lat pozbawienia wolności (Skelnik, 2018).

Warto zatem pamiętać jak bardzo ważna jest ochrona naszych danych osobowych i jak bardzo władze starają się nie dopuścić do ich wycieków. Myślę, że wprowadzenie RODO jest genialnym pomysłem, zwłaszcza teraz, gdy mamy erę Internetu i często nie zdajemy sobie sprawy, jak bardzo łatwo jest włamać się do baz danych. Oszuści mogą o nas wiedzieć praktycznie wszystko, a my możemy nie być nawet świadomi tego, jak w tym czasie wykorzystują nasze dane. Dlatego warto być czujnym, a wszelkie wątpliwości natychmiast zgłaszać. Zbyt późne reakcje mogą doprowadzić do poważnych problemów.

Bibliografia

Kompendium wiedzy na temat RODO. Pobrane z: https://odo24.pl/rodo.

Podstawowe zagadnienia dotyczące ochrony danych osobowych (z testem). (2014). Pobrane z: http://isp.policja.pl/isp/aktualnosci/4703,Podstawowe-zagadnienia-dotyczace-ochrony-danych-osobowych-z-testem.html.

Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Dz.U. UE L 119/1.

Skelnik, K. (2018). *Dane w sieci — czy wymogi RODO zmienią ich zabezpieczenie?*. Pobrane z: http://centrumprasowe.wsb.pl/30008-dane-w-sieci-czy-wymogi-rodo-zmienia-ich-zabezpieczenie.

Ustawa z dnia 10 czerwca 2016 r. o działaniu antyterrorystycznym. Dz.U. poz. 904.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. z 2016 r. poz. 922.

Ustawa z dnia 6 kwietnia 1990 r. o Policji. Dz.U. z 2017 r., poz. 2067.

The implementation of General Data Protection Regulation

Abstract

The General Data Protection Regulation (GDPR), as a recently popular theme, evokes mostly negative emotions. A lot of unfavorable comments have been voiced, so it is also a topic reluctantly approached. The article allows for a different view on GPDR, shows where the focus on personal data protection is placed and what the consequences of not following the regulations are.

Keywords: GPDR, safety, data, protection.