EBIB Biuletyn EBIB, nr 4 (181)/2018,
Zarządzanie bibliotekami – aspekty prawne
Artykuły

Mirosław Rostkowski
Urząd Miasta w Chełmży
mirekrostkowski@interia.pl

Nowe zasady ochrony danych osobowych – kilka refleksji nt. RODO

Streszczenie: Z dniem 25 maja 2018 r. weszły w życie nowe przepisy w zakresie ochrony danych osobowych. Rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, tzw. RODO, ma chronić prywatność informacyjną jednostki w relacji z silniejszymi podmiotami. W artykule dokonano próby wyjaśnienia, czym jest RODO, scharakteryzowano jego cechy, takie jak: ogólnikowość, mierzalność, bezpośredniość, surowość i domniemanie winy.

Słowa kluczowe: RODO, dane osobowe, ochrona danych osobowych

Obowiązujące od 25 maja 2018 r. nowe przepisy w zakresie ochrony danych osobowych od samego początku spotykają się z dużym niezrozumieniem i brakiem przychylności, o czym świadczy chociażby liczba zgłoszeń do Urzędu Ochrony Danych Osobowych w tak krótkim okresie stosowania RODO[1] – około 600 zapytań i około 750 naruszeń. Chociaż przepisy dotyczące ochrony danych osobowych weszły w życie w 1997 r., to w dalszym ciągu ich stosowanie i przestrzeganie budzi wiele pytań i kontrowersji. Często można się spotkać ze sceptyczną postawą, czy ochrona danych osobowych jest potrzebna, skoro i tak nasze dane znajdują się już gdzieś w przestrzeni publicznej i są używane w różnych celach, nie zawsze zgodnie z przepisami. I właśnie po to, aby zapobiec takim praktykom, powinno się stosować przepisy o ochronie danych osobowych.

RODO ma chronić prywatność informacyjną jednostki w relacji z podmiotami silniejszymi, ma stanowić swego rodzaju zaporę przed wykorzystywaniem danych osobowych do różnych celów bez wiedzy i udziału tych osób. W motywie pierwszym Preambuły rozporządzenia ustanowiono, że ochrona osób fizycznych w związku z przetwarzaniem danych osobowych należy do praw podstawowych, a każdy ma prawo do ochrony danych osobowych jego dotyczących.

Wdrożenie RODO nie jest łatwe – od instytucji przetwarzających dane osobowe (administratorów tych danych) wymaga dokładnego zapoznania się z rozporządzeniem oraz ustawą, opracowania i stosowania klauzuli zgody na przetwarzanie danych, klauzuli informacyjnej i różnych innych procedur, a także zatrudnienia inspektora ochrony danych osobowych.

Uchwalona 10 maja 2018 r. ustawa o ochronie danych osobowych[2] w art. 1 ust. 2 określa podmioty publiczne zobowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o jego wybraniu. W art. 9 ustawy wyjaśniono, że przez organy i podmioty

[1] *Rozporządzenie Parlamentu Europejskiego i Rady Europy (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 osobowych).*
[2] *Ustawa z 10 maja 2018 r . o ochronie danych osobowych.* Dz.U. 2018, poz. 1000.

publiczne zobowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a RODO, rozumie się:

1) jednostki sektora finansów publicznych,
2) instytuty badawcze,
3) Narodowy Bank Polski.

Ustawa o finansach publicznych[3] w art. 9 wymienia podmioty tworzące sektor finansów publicznych, a w punkcie 13 tego artykułu wymienia państwowe i samorządowe instytucje kultury. Tak więc zgodnie z powyższym do wyznaczenia inspektora ochrony danych osobowych zobowiązane są także biblioteki publiczne będące państwowymi lub samorządowymi instytucjami kultury. Ze względu na zakres przetwarzania danych i specyficzne warunki organizacyjne, dyrektorzy bibliotek i bibliotekarze powinni dołożyć wszelkich starań, aby powierzone im przez czytelników dane osobowe były chronione zgodnie z rozporządzeniem.

Najogólniej RODO można określić jako trudne, pouczające, niezrozumiałe i surowe. Jednakże po dokonaniu głębszej analizy można stwierdzić, że rozporządzenie jest przede wszystkim wymagające, a ustanowione w nim zasady ochrony danych osobowych są ogólnikowe, mierzalne, bezpośrednie i surowe[4]. Charakterystyczna dla rozporządzenia jest także zasada domniemania winy. Poniżej w dużym skrócie dokonano próby wyjaśnienia wymienionych cech RODO.

Ogólnikowość przejawia się w szczególności w art. 5, zgodnie z którym przy przetwarzaniu danych osobowych należy kierować się następującymi zasadami:

1. Legalnością, czyli przetwarzanie powinno się odbywać w oparciu o podstawę prawną. W rozporządzeniu w art. 6 znajdują się przesłanki prawne do przetwarzania danych osobowych zwykłych, natomiast w art. 9 do przetwarzania danych szczególnych.
2. Rzetelnością, czyli przetwarzanie powinno odbywać się uczciwie, w dobrej wierze, bez wprowadzania w błąd.
3. Przejrzystością, czyli czytelnie, z prostotą i zrozumieniem.
4. Konkretnością, czyli z ograniczeniem zakresu przetwarzanych danych do realizacji danego celu.
5. Minimalizacją danych, to znaczy, że należy gromadzić tylko dane, które są niezbędne do realizacji celu.
6. Dbałością o to, aby gromadzone dane osobowe były poprawne i aktualne.
7. Minimalizacją czasu ich przetwarzania, to znaczy, że dane należy przetwarzać do momentu zakończenia realizacji celu i zgodnie z ograniczeniem czasowym wynikającym z przepisów prawa w tym zakresie.
8. Bezpieczeństwem, zapewniając przetwarzanym danym osobowym poufność, integralność i dostępność.

W całym rozporządzeniu można się spotkać ze sporymi uogólnieniami stanowionych przepisów, ogólnymi wskazaniami, bez sprecyzowania chociażby, co oznacza duża skala przetwarzania – czy to jest przetwarzanie danych 50, 100 czy może większej liczby osób,

[3] *Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych.* Tekst jedn. Dz.U. 2017, poz. 2077, z późn. zm.
[4] GAWROŃSKI, M. (red.). *RODO: przewodnik ze wzorami*. Warszawa: Wolters Kluwer, 2018. ISBN 9788381246378.

czy jak spełnić wymagania bezpiecznego przetwarzania danych osobowych, jakie zastosować rozwiązania organizacyjne i techniczne.

Niejako przeciwieństwem do ogólnikowości jest **mierzalność**. W tym przypadku mamy do czynienia z jasno sprecyzowanymi i mierzalnymi terminami. Gdy dana osoba zwróci się do administratora o udostępnienie informacji na temat celu i zakresu przetwarzania jej danych osobowych, lub z żądaniem usunięcia tych danych, administrator w ciągu miesiąca musi udzielić odpowiedzi na zadane pytania. Termin ten może zostać przedłużony maksymalnie o dwa miesiące, ale o przyczynach i przedłużeniu należy poinformować zainteresowaną osobę w ciągu miesiąca. Jeżeli w organizacji wskutek jakiegoś incydentu dojdzie do naruszenia ochrony danych osobowych, administrator musi o tym fakcie powiadomić organ nadzorczy (Urząd Ochrony Danych Osobowych) w ciągu 72 godzin od momentu powzięcia informacji o naruszeniu.

Kierując się zasadą **mierzalności**, administrator musi przestrzegać określonych terminów nałożonych przez prawo, by wykonać ciążące na nim obowiązki. Aby temu sprostać, powinien posiadać dobrze przeszkolony personel, opracowane procedury i opisane zasady współpracy z podmiotami, którym powierza przetwarzanie danych osobowych.

Chcąc sprostać obowiązkom nałożonym na administratorów, dyrektorzy i pozostali pracownicy bibliotek powinni zgodnie z zasadą rozliczalności mieć opracowaną politykę ochrony danych osobowych, w której należy określić: warunki organizacyjne i techniczne przetwarzania danych osobowych, stosowane zabezpieczenia, reguły zarządzania systemami informatycznymi, wzory klauzuli zgody, klauzuli informacyjnej, upoważnienia do przetwarzania danych osobowych oraz wzór umowy powierzenia danych osobowych. Jednym z ważniejszych dokumentów, który stanowi swego rodzaju mapę przetwarzanych danych osobowych w bibliotece, jest rejestr czynności przetwarzania, który zawiera wykaz wszystkich czynności wymagających przetwarzania danych osobowych w organizacji. Powinien on zawierać m.in. sprawy kadrowe, sprawy związane z organizowaniem działalności kulturalnej mieszkańców (np. gminy), obsługę czytelników czy realizację prawa dostępu do informacji publicznej. W tym miejscu warto przypomnieć, że to administrator uprawnia pracowników do przetwarzania danych osobowych, wydając im odpowiednie upoważnienia po przeprowadzeniu szkolenia.

Bezpośredniość związana jest z obowiązkiem stosowania rozporządzenia we wszystkich państwach Unii Europejskiej. Rozporządzenie stanowi nową ustawę o ochronie danych osobowych, służącą jego stosowaniu.

Surowość można rozumieć jako stosowanie konkretnych kar za nieprzestrzeganie przepisów prawa o ochronie danych osobowych i naruszeniem ich postanowień. Zgodnie z art. 83 RODO kary powinny być skuteczne, proporcjonalne i odstraszające. Wymienia się możliwość stosowania kar pieniężnych na dwóch poziomach: do 10 mln euro i do 20 mln euro. Jednakże zgodnie z art. 102 na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy o finansach publicznych, do których należą także biblioteki, Prezes Urzędu może nałożyć w drodze decyzji administracyjnej kary pieniężne w wysokości do 10 000 złotych.

Ostatnią cechą określającą całą złożoność RODO jest **domniemanie winy**. Duża ogólność stanowionych przepisów rozporządzenia wymaga od administratora stosowania

zasady rozliczalności, która jest fundamentem RODO. Chroniąc się przed przypisaniem domniemania winy, organizacja i jej administrator muszą być w stanie wykazać (rozliczyć się), że przestrzegają przepisów i stosują reguły chroniące powierzone im dane osobowe przez konkretne osoby. W art. 5 ust. 2 RODO ustanowiono, że administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać przed organem nadzorczym, że ich przestrzega (rozliczalność). Natomiast art. 82 ust. 3 RODO stanowi, że administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

Charakteryzując ogólną ideę rozporządzenia, należy stwierdzić, że nowy system ochrony danych osobowych wymusza na organizacjach i podmiotach dostosowanie procesów przetwarzania danych osobowych nie tylko pod względem prawnym, ale również w zakresie organizacyjnym, technicznym, technologicznym i mentalnym.

Administratorzy niedużych instytucji, do których należy zaliczyć biblioteki gminne, są zobowiązani do stosowania przepisów rozporządzenia w takim samym zakresie jak organizacje większe czy organizacje korporacyjne. Aby sprostać wszystkim wymaganiom, dyrektor biblioteki, który jest administratorem danych, musi dogłębnie przestudiować obowiązujące przepisy, tj. rozporządzenia i ustawy. Następnie powinien wprowadzić politykę ochrony danych do stosowania w organizacji. W kolejnym kroku powinien przeanalizować, na ile posiadana infrastruktura informatyczna spełnia warunki bezpiecznego przetwarzania danych.

Z przeprowadzonej w wielu organizacjach oceny ryzyka wynika, że najsłabszym ogniwem w systemie bezpieczeństwa ochrony danych osobowych w zakresie praw i wolności osoby fizycznej jest czynnik ludzki. Wobec tego ten właśnie obszar bezpieczeństwa wymaga szczegółowej analizy oraz zaimplementowania działań profilaktycznych i kontrolnych. Dlatego też budowanie skutecznego systemu ochrony praw i wolności wymaga, obok wdrażania nowych zabezpieczeń, także podnoszenia ogólnej świadomości pracowników w tym zakresie, np. za pośrednictwem cyklicznie organizowanych szkoleń.

Bibliografia:

1. GAWROŃSKI, M. (red.). *RODO: przewodnik ze wzorami*. Warszawa: Wolters Kluwer, 2018. ISBN 9788381246378.
2. *Rozporządzenie Parlamentu Europejskiego i Rady Europy (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 osobowych).*
3. *Ustawa z 10 maja 2018 r. o ochronie danych osobowych.* Dz.U. 2018, poz. 1000.
4. *Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych.* Tekst jedn. Dz.U. 2017, poz. 2077, z późn. zm.

ROSTKOWSKI, M. Nowe zasady ochrony danych osobowych – kilka refleksji nt. RODO. *Biuletyn EBIB* [online] 2018, nr 4 (181), Zarządzanie bibliotekami – aspekty prawne. [Dostęp 25.08.2018]. ISSN 1507-7187. Dostępny w: http://open.ebib.pl/ojs/index.php/ebib/article/view/650.