Ekonomiczne Problemy Usług nr 2/2018 (131), t. 1

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2018.131/1-30 | strony: 303–313

Stefan Rozmus
Wojskowa Akademia Techniczna
Wydział Cybernetyki
Instytut Systemów Informatycznych
Zakład Inżynierii Systemów Informatycznych
stefan.rozmus@wat.edu.pl

E-learning w świetle RODO

Kody JEL: I21, K390
Słowa kluczowe: RODO, dane osobowe, e-learning, platforma e-learning
Streszczenie. Od dwudziestego piątego maja 2018 roku w państwach Unii Europejskiej zacznie obowiązywać Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO). Rozporządzenie będzie spójnym narzędziem do stosowania we wszystkich państwach członkowskich, zastępującym dotychczasowe regulacje prawne dotyczące ochrony danych osobowych poszczególnych państw Unii. Celem niniejszej pracy jest wskazanie najważniejszych zmian, wprowadzanych przepisami RODO, które zdaniem autora powinny zostać uwzględnione w procesie identyfikacji istniejących niezgodności i luk w zakresie ochrony danych osobowych, w odniesieniu do e-learningu.

Wprowadzenie

Wykorzystanie e-learningu jako formy kształcenia na uczelni wyższej nabiera w ostatnich latach coraz większego znaczenia. Wynika to z faktu, że studenci, również studiujący w trybie studiów dziennych, chcą lub są zmuszeni łączyć naukę z pracą zawodową. Dotyczy to głównie studentów ostatnich lat studiów, gdyż jest to bardzo dobry moment, a dla niektórych najwyższy czas, na rozpoczęcie kariery zawodowej (Skwarka, Jargiło, Łasocha, 2012, s. 6). Niezależnie od formy zatrudnienia (praca na część lub na cały etat, własna działalność gospodarcza czy też praca na umowę o dzieło lub zlecenie) systematyczny udział pracujących studentów w zajęciach, prowadzonych w tradycyjny

sposób[1], jest utrudniony, a niejednokrotnie wręcz niemożliwy. Również z obserwacji autora podczas prowadzonych zajęć dydaktycznych na ostatnich latach studiów, a także z rozmów, przeprowadzonych z nauczycielami akademickimi różnych uczelni wynika, że frekwencja studentów na tego typu zajęciach corocznie maleje. Szczególnie widoczny jest nikły udział studentów w zajęciach nieobowiązkowych, który niekiedy nie przekracza kilku procent.

W tej sytuacji e-learning jawi się jako skuteczne rozwiązanie zaistniałego problemu. Posiada bowiem niekwestionowane zalety, takie jak możliwość przyswajania wiedzy przez studenta w dogodnym w zaistniałej sytuacji dla niego czasie[2] i miejscu, w akceptowalnym przez niego tempie bez niepotrzebnej presji czasowej, czy też wielokrotnego powtarzania materiału. E-learning jest z reguły tańszy zarówno z punktu widzenia samej uczelni, jak i studenta. Ponadto, jeżeli uwzględnimy, że potwierdzanie części uczenia się można przeprowadzić również za pośrednictwem platformy e-learningowej, czyli bez konieczności osobistego stawiennictwa studenta na uczelni[3], można stwierdzić, że ta forma kształcenia wychodzi naprzeciw potrzebom pracujących studentów. Ale nie tylko. E-learning to idealna propozycja także dla osób już aktywnych zawodowo, którym trudno pogodzić pracę z planem zajęć na uczelni (nawet w przypadku studiów wieczorowych) oraz wszystkim innym, którzy rezygnują ze studiów z powodu braku czasu na regularne uczęszczanie na zajęcia. Istotnym jest również fakt, że aktualne uregulowania prawne sprzyjają rozwojowi e-learningu. Zezwalają bowiem na realizację nawet do 80% ogólnej liczby godzin zajęć dydaktycznych, określonych w standardach kształcenia dla poszczególnych kierunków studiów oraz poziomów kształcenia[4], na studiach stacjonarnych i niestacjonarnych, prowadzonych z wykorzystaniem metod i technik kształcenia na odległość (Dz.U 2007, poz. 1347, § 5).

Pomimo tego, że jeszcze nie tak dawno większość zajęć na uczelniach odbywała się w tradycyjny sposób (Hołowiecki, 2014, s. 205), a jakość i skuteczność kształcenia w formie e-learningu nadal pozostaje nierozwiązaną kwestią, nie zmienia to faktu, że jest to innowacyjna koncepcja rozwoju, pozwalająca na zdobycie cennego doświadczenia, która w przyszłości będzie jeszcze bardziej rozwijana (Sadłowski, 2017, s. 50).

Trzymając się tej tezy, konieczne jest zwrócenie bacznej uwagi na jeden z istotnych aspektów e-learningu, niemający bezpośredniego związku z samym e-learningiem jako formą kształcenia. Chodzi mianowicie o ochronę danych osobowych[5]. Przyjęte przez Parlament Europejski i Radę Unii Europejskiej w 2016 roku Rozporządzenie

---

[1] Chodzi tu o wszelkie formy zajęć prowadzonych bezpośrednio na uczelni.

[2] Jedynym ograniczeniem będą tutaj z góry ustalone przez uczelnię terminy zaliczeń, egzaminów oraz rozliczania się z prac kontrolnych.

[3] Aktualnie w większości uczelni część zaliczeń, a także egzaminy, odbywają się w trakcie tzw. zjazdów, w których uczestnictwo jest obowiązkowe.

[4] Z wyłączeniem zajęć praktycznych i laboratoryjnych.

[5] E-learning, ze swej natury, bazuje na platformach e-learningowych będących systemami informatycznymi, w których przetwarzane są dane osobowe studentów i wykładowców.

Ogólne o Ochronie Danych Osobowych (zwane dalej RODO), w nieodległym czasie zastąpi dotychczasowe regulacje prawne dotyczące ochrony danych osobowych obowiązujące w poszczególnych państwach Unii Europejskiej. RODO, które w swym zamierzeniu ma być spójnym narzędziem do stosowania we wszystkich państwach członkowskich Unii, zacznie obowiązywać już od 25 maja 2018 roku. Do tego czasu niezbędne jest dostosowanie dotychczasowych przepisów dotyczących ochrony danych osobowych tak, aby spełniały wymagania stawiane przez RODO. Trzeba tu wyraźnie podkreślić, że brak spełnienia tych wymagań będzie skutkował znacznie poważniejszymi konsekwencjami, w tym materialnymi, niż w dotychczas obowiązujących przepisach prawa.

Celem niniejszej pracy jest wskazanie najważniejszych zmian, wprowadzanych przepisami RODO, które zdaniem autora powinny zostać uwzględnione w procesie identyfikacji istniejących niezgodności i luk w zakresie ochrony danych osobowych, w odniesieniu do e-learningu. Proces ten powinien w szczególności objąć weryfikację dokumentacji, procedur organizacyjnych oraz eksploatowanych platform e-learningowych w celu określenia, a następnie podjęcia, niezbędnych działań dostosowawczych.

1. Wpływ zmian w definicjach pojęć na aktualne przepisy krajowe dotyczące ochrony danych osobowych

Rozporządzenie Ogólne o Ochronie Danych Osobowych zawiera szereg definicji pojęć wykorzystywanych tym w rozporządzeniu (RODO, 2016, art. 4), z których pewna część stanowi nowość, natomiast inne, w większym bądź mniejszym stopniu, uległy modyfikacji w stosunku do dotychczasowego stanu prawnego[6]. Zrozumienie wprowadzonych definicji ma kluczowe znaczenie dla podejmowania dalszych działań, ponieważ sprzeczna z przepisem prawa unijnego norma krajowa nie może być zastosowana[7].

Zajmująca, ze względów oczywistych, pierwszą pozycję definicja pojęcia danych osobowych, w zasadniczej części nie uległa zmianie w stosunku obowiązujących przepisów o ochronie danych osobowych. **Dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną,

[6] Wykazywane w definicjach pojęć zmiany odnoszą się do odpowiadających im zapisów w ustawie o ochronie danych osobowych z dnia 29 sierpnia 1997 r. Dz.U. 2016, poz. 922.

[7] Wynika to z podstawowych zasad prawa europejskiego, w szczególności z zasady pierwszeństwa, zgodnie z którą prawo europejskie jest nadrzędne w stosunku do prawa krajowego państw członkowskich.

genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (RODO, 2016, art. 4 ust. 1). Natomiast widoczne jest tutaj rozszerzenie wykazu przykładów danych osobowych, w szczególności w odniesieniu do danych elektronicznych, takich jak dane o lokalizacji czy też identyfikator internetowy.

Podobny zakres zmian odnosi się do definicji pojęcia **przetwarzanie**, którego dotychczasowym odpowiednikiem jest „przetwarzanie danych". Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (RODO, 2016, art. 4 ust. 2). Z definicji jednoznacznie wynika, że przetwarzanie dotyczy danych osobowych. Ujęte w definicji przykłady czynności powinny ułatwić stosowanie w praktyce ogólnej definicji przetwarzania.

Zmiana, która z pewnością skomplikuje dostosowanie obecnych przepisów do wymogów RODO, dotyczy definicji pojęcia **odbiorca**. Z definicji, odbiorca oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (RODO, 2016, art. 4 ust. 9). Zatem osoby posiadające upoważnienie do przetwarzania danych osobowych, nadane im przez administratora[8], również należy uznać za odbiorców (w myśl obecnych przepisów, osoby te nie są odbiorcami, podobnie jak osoby, których dane dotyczą). Przede wszystkim należy wskazać, że przyjęcie koncepcji, w której odbiorcą danych jest także osoba funkcjonująca w strukturze administratora, prowadzi do znacznego utrudnienia realizacji obowiązków przez administratora, a jednocześnie nie wzmacnia praw osób, których dane dotyczą (Bielak-Jomaa, Lubasz, 2018, s. 234–235).

Nowością jest definicja pojęcia **pseudonimizacja**. Pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (RODO, 2016, art. 4 ust. 5). Celem pseudonimizacji jest utrudnienie identyfikacji konkretnej osoby fizycznej przy jednoczesnym zachowaniu możliwości ustalenia jej tożsamości w przypadku wykorzystania dodatkowych informacji. Pseudonimizacja wskazana jest jako jeden ze środków technicznych i organizacyjnych, z których może skorzystać administrator, aby zapewnić

[8] Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (RODO, 2016, art. 4 ust. 7).

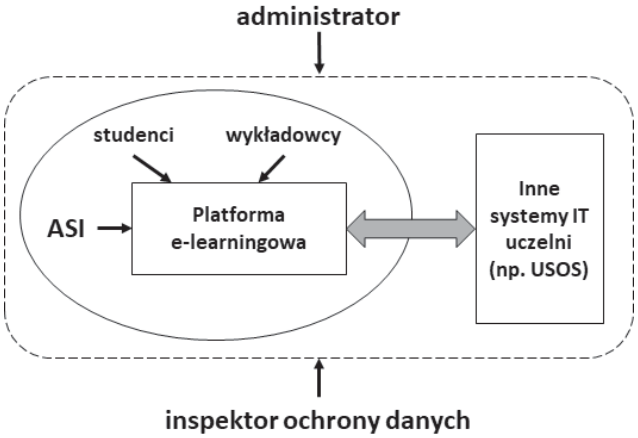
stopień bezpieczeństwa adekwatny do zidentyfikowanego ryzyka (RODO, 2016, art. 32 ust. 1 lit. a).

Wprowadzone przez RODO pojęcie **naruszenie ochrony danych osobowych** nie znajduje swojego odzwierciedlenia w obecnym stanie prawnym[9]. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (RODO, 2016, art. 4 ust. 12). Zapisy ujęte w definicji mają istotny wpływ na regulację obowiązków administratora związanych zarówno ze zgłaszaniem naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, jak i zawiadamianiem osób, których dane dotyczą, o takim naruszeniu.

2. E-learning a ochrona danych osobowych zgodna z RODO

Realizacja ustawowych zadań przez uczelnię wyższą (Dz.U. 2017, art. 13 ust. 1) ze swej natury wymaga przetwarzania danych osobowych pracowników oraz studentów. Wdrożenie e-learningu to nic innego, jak udostępnienie specjalistycznego środowiska teleinformatycznego (platformy e-learningowej), w którym odbywać się będzie przetwarzanie pewnego podzbioru tych danych osobowych. Zatem posiadanie platformy e-learningowej wiąże się z szeregiem obowiązków wynikających z przepisów prawa, nałożonych zarówno na osoby mające do niej bezpośredni dostęp, jak i na odpowiedzialne za właściwą ochronę danych osobowych na uczelni. Tak rozumiane otoczenie platformy e-learningowej widziane z perspektywy RODO (rys. 1) uległo pewnym zmianom w stosunku do dotychczas obowiązujących przepisów. I nie chodzi tu tylko o usankcjonowanie nowej roli, roli inspektora ochrony danych (OID), który zastąpi funkcjonującego dotychczas administratora bezpieczeństwa informacji (ABI).

[9] Ustawa o ochronie danych osobowych posługuje się pojęciem naruszenia przepisów o ochronie danych osobowych, jednak nie jest ono analogiczne do naruszenia ochrony danych osobowych na gruncie RODO.



Rysunek 1. Otoczenie platformy e-learningowej w perspektywie RODO

Źródło: opracowanie własne.

RODO nie przewiduje wyznaczania zastępców inspektora ochrony danych, jak to ma miejsce w odniesieniu do administratorów bezpieczeństwa informacji (Dz.U. 2016a, art. 31a ust. 6). W tym kontekście zachowanie możliwości wyznaczania odpowiedników dotychczas powoływanych lokalnych administratorów bezpieczeństwa informacji (LABI) wymaga rozwiązań prawnych na poziomie krajowym. Podobnie, konieczne jest znalezienie rozwiązania zezwalającego na delegowanie uprawnień administratora na szczebel podstawowych jednostek organizacyjnych, co zapewniłoby utrzymanie dotychczasowej roli lokalnego administratora danych osobowych (LADO)[10]. Podstawą do podjęcia działań w tym zakresie[11] jest fakt, że RODO nie wyklucza możliwości określenia w prawie państwa członkowskiego okoliczności dotyczących konkretnych sytuacji związanych z przetwarzaniem danych, w tym dookreślenia warunków, które decydują o zgodności przetwarzania z prawem (RODO, 2016, s. 2). Należy przy tym uwzględnić rozszerzone obowiązki przypisywane poszczególnym rolom, ujęte w RODO.

Administrator odpowiada za wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających zgodność przetwarzania z wymogami RODO. Cho-

[10] Niewłaściwym byłoby bazowanie na definicji pojęcia **przedstawiciel**, które znajdzie zastosowanie wyłącznie w przypadkach, w których administrator niemający jednostki organizacyjnej w Unii Europejskiej przetwarzać będzie dane osobowe osób znajdujących się w Unii (Bielak-Jomaa, Lubasz, 2018, s. 286).

[11] Zapewnianie i nadzorowanie przestrzegania zasad ochrony przetwarzania danych osobowych w oparciu o administratorów lokalnych (odpowiednio – LADO i LABI) jest powszechnie stosowaną praktyką w uczelniach o złożonej strukturze organizacyjnej. Zdaniem autora, pozostawienie tego stanu rzeczy leży w interesie administratora.

dzi tu w szczególności o realizację zasad wskazanych w rozporządzeniu, tj. zasady zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności (RODO, 2016, art. 5 ust. 1). Dobór środków i zakresu zabezpieczeń wdrażanych przez administratorów nie powinien mieć charakteru jednolitego, niezależnego od zakresu, formy, celu i ilości przetwarzanych danych, lecz musi być związany z oceną dokonywaną przez administratora w zakresie ryzyka oraz wpływu przetwarzania na prywatność. Jest to istotna nowość w stosunku do aktualnego stanu prawnego. Jeżeli doliczyć do tego kolejne nowe obowiązki, tzn. obowiązki uwzględniania ochrony danych już w fazie projektowania oraz w drodze realizacji zasady domyślnej ochrony danych[12], to nie ulega wątpliwości, że obecne polityki bezpieczeństwa przetwarzania danych osobowych muszą zostać zmienione.

Inspektor ochrony danych (IOD) musi być zawsze wyznaczony, gdy przetwarzania dokonuje organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości (RODO, 2016, art. 37 ust. 1). Stąd administrator w uczelni publicznej ma obowiązek wyznaczenia IOD[13]. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia co najmniej następujących zadań (RODO, 2016, art. 39 ust. 1):

- informowanie administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie,
- monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.

Podobnie, jak w przypadku administratora, RODO wyraźnie zobowiązuje inspektora ochrony danych do wykonywania swoich zadań z należytym uwzględnieniem ry-

---

[12] Stanowi to odejście od modelu reaktywnej ochrony prywatności na rzecz ochrony proaktywnej, obejmującej cały cykl życia informacji.

[13] Wprawdzie RODO nie definiuje pojęcia organu ani podmiotu publicznego, ale można w tym przypadku oprzeć się na zapisach ustawy o finansach publicznych (Dz.U. 2016b, art. 9 pkt. 1–14), w której uczelnia publiczna została zaliczona w poczet podmiotów publicznych.

zyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania (RODO, 2016, art. 39 ust. 2). Wiąże się to z koniecznością indywidualnego i samodzielnego określania środków i metod działania oraz dostosowywania ich do specyfiki konkretnego administratora. Zatem należy stwierdzić, że, w ogólnym przypadku, szeroka rzesza obecnych administratorów i ABI będzie zmuszona do uzupełnienia swoich kompetencji o zarządzanie ryzykiem, aby sprostać przyszłym zadaniom.

Odnosząc się do faktycznych użytkowników platformy e-learningowej (studenci i wykładowcy) należy zaznaczyć, że w myśl obecnych przepisów do przetwarzania danych osobowych studentów w ramach e-learningu uprawnieni są tylko wykładowcy, którzy posiadają stosowne upoważnienie do przetwarzania tych danych, wydane przez LADO. Zgodę na przetwarzanie swoich danych osobowych przez uczelnię, w zakresie niezbędnym do zapewnienia prawidłowego toku studiów, każdy student podpisuje na kwestionariuszu składanym przez kandydata ubiegającego się o przyjęcie na studia. W ramach e-learningu student ma dostęp wyłącznie do swoich danych osobowych.

RODO nie określa obowiązków administratora danych co do konkretnych rozwiązań, jakie należy wdrożyć w ramach procedur bezpieczeństwa informacji, w szczególności nie odnosi się wprost do rzeczonych upoważnień. Niemniej jednak wprowadza wymóg, aby każda osoba działająca z upoważnienia administratora i mająca dostęp do danych osobowych przetwarzała je wyłącznie na polecenie administratora (RODO, 2016, art. 29). Należy zatem przyjąć, że administrator w odpowiedni sposób upoważnia swoich pracowników (w tym przypadku wykładowców) do przetwarzania danych osobowych. I to jest kolejne zagadnienie do unormowania w ramach nowelizacji ustawy o ochronie danych osobowych, nad którą nadal trwają prace (MC, 2018).

Pozostaje jeszcze odniesienie się do roli ASI (rys. 1), czyli administratora systemu informatycznego. Co ciekawe, ani obecnie obowiązujące regulacje w zakresie ochrony danych osobowych nie przewidywały, ani RODO nie przewiduje powołania takiego stanowiska. A jednak ASI funkcjonuje obecnie i, zdaniem autora, pozostanie po wejściu w życie RODO. Jak pokazuje praktyka, osoba pełniąca funkcję ABI w organizacji bardzo często nie posiada wystarczających kompetencji w zakresie wdrażania i utrzymania systemów teleinformatycznych[14]. Stąd pojawienie się ASI, który z założenia takie kompetencje powinien posiadać, i który współpracując z ABI, powinien sprawować ogólny nadzór nad bezpieczeństwem organizacyjnym, oraz technicznym, pod kątem infrastruktury teleinformatycznej[15]. Wydaje się, że zasadnym byłoby umocowanie ASI w znowelizowanej ustawie o ochronie danych osobowych.

---

[14] Zgodnie z RODO kompetencje te muszą obejmować również wiedzę i umiejętności uwzględniania ochrony danych już w fazie projektowania systemu teleinformatycznego (o czym wspomniano już wcześniej).

[15] W uczelni publicznej może funkcjonować więcej niż jeden ASI, w szczególności, gdy administrator powołał lokalnych administratorów danych osobowych na poziomie podstawowych jednostkach organizacyjnych, np. na każdym z wydziałów.

4. Sankcje

Analizując wpływ RODO na e-learning nie można pominąć aspektu sankcji, które grożą za naruszenie przepisów o ochronie danych osobowych. Daje temu dowód MC (2018) stwierdzając, że „[d]o zagadnień podlegających regulacji w nowo tworzonym prawie ochrony danych osobowych będą należały w szczególności: (…) kary niezbędne dla zapewnienia efektywnego wykonywania nadzoru".

W myśl nowych przepisów (RODO, 2016, art. 83) za naruszenia przepisów wynikających z RODO nakładane są administracyjne kary pieniężne, które mają być w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające. Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku. I tak, przykładowo, za:

- naruszenie obowiązków administratora grozi kara administracyjna do 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa,
- nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy grozi kara administracyjna w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Ponadto, co wynika z RODO (2016, art. 84 ust. 1), państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenia RODO, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym, oraz podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające[16].

Podsumowanie

Wprowadzenie nowych, jednolitych dla państw członkowskich Unii Europejskiej, regulacji prawnych dotyczących ochrony danych osobowych, określonych w RODO, nie pozostaje bez wpływu na aktualnie obowiązujące w tym zakresie przepisy prawa poszczególnych państw członkowskich. Ze względu na ogólność części zapisów w RODO, wystąpiła konieczność ich doprecyzowania w odpowiednich krajowych normach prawnych tak, aby nie zostały one naruszone. Nie jest to zadanie łatwe. Świadczy o tym aktualny stan prac nad nowelizacją ustawy o ochronie danych osobowych (MC, 2018), które nie zostały jeszcze zakończone pomimo świadomości, że czasu pozostało coraz mniej (rys. 2).

[16] Do dnia 25 maja 2018 r. każde państwo członkowskie zobowiązane jest do zawiadomienia Komisji Europejskiej o swoich przepisach przyjętych w tym zakresie, a następnie niezwłocznie o każdej późniejszej ich zmianie.

Rysunek 2. Odliczanie dni do RODO

Źródło: http://giodo.gov.pl/560/id_art/9121/j/pl (4.02.2018).

Poruszone w pracy zagadnienia to tylko część problemów, które dotykają e-learning z powodu nieodległego wejścia w życie obowiązku przestrzegania przepisów zawartych w RODO. Biorąc pod uwagę narzucone ograniczenia co do rozmiaru pracy, zostały w niej przedstawione najważniejsze, zdaniem autora[17], zmiany, które powinny zostać uwzględnione w procesie identyfikacji istniejących niezgodności i luk w zakresie ochrony danych osobowych, w odniesieniu do e-learningu.

Na zakończenie autor pragnie wyrazić nadzieję, że zanim licznik (rys. 2) zostanie wyzerowany, uczelnie zdążą wdrożyć zmienione przepisy na swoim, lokalnym gruncie. Konferencja[18], rozpoczynająca się w przeddzień wejścia w życie RODO, będzie właściwym miejscem do weryfikacji, na ile ta nadzieja została spełniona.

Literatura

Bielak-Jomaa, E., Lubasz, D. (red.) (2018). *RODO. Ogólne Rozporządzenie o Ochronie Danych. Komentarz*. Warszawa: Wolters Kluwer.

Dz.U. (2007). Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 25 września 2007 r. w sprawie warunków, jakie muszą być spełnione, aby zajęcia dydaktyczne na studiach mogły być prowadzone z wykorzystaniem metod i technik kształcenia na odległość. Dz.U. 2007 nr 188, poz. 1347.

Dz.U. (2016b). Ustawa z dnia 27 sierpnia 2016 r. o finansach publicznych. Dz.U. 2016, poz. 1870.

Dz.U. (2017). Ustawa z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym. Dz.U. 2017, poz. 2183.

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

Hołowiecki, M. (2014). Wykorzystanie e-learningu jako formy kształcenia zdalnego na publicznych uczelniach wyższych w Polsce. *Lingua ac Communitas*, *24*, 185–206.

[17] Autor pełni aktualnie funkcję LABI w Centrum Studiów Zaawansowanych Inżynierii Systemów Wydziału Cybernetyki WAT i jest odpowiedzialny za wdrożenie nowej platformy e-learningowej.

[18] Konferencja „Cywilizacja informacyjna i jej oddziaływanie na transformację gospodarczą i społeczną" Szczecin – Kopenhaga 22–25.05.2018 r., na którą zgłoszono niniejszą pracę.

https://repozytorium.amu.edu.pl/bitstream/10593/13158/1/lingua_ac_communitas_vol_24_2014-Holowiecki.pdf (25.01.2018).

http://giodo.gov.pl/560/id_art/9121/j/pl (4.02.2018).

MC (2018). *Nowe prawo ochrony danych osobowych. Ministerstwo Cyfryzacji*. Pobrano z: https://www.gov.pl/cyfryzacja/nowe-prawo-ochrony-danych-osobowych (3.02.2018).

RODO (2016). 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. Urz. UE L 119/1, 4.05.2016.

Sadłowski, R. (2017). Współczesny E-learning na wyższych uczelniach w opinii osób studiujących. *Rynek – Społeczeństwo – Kultura*, *1* (22), 49–53. Pobrano z: http://www.kwartalnikrsk.pl/assets/rsk1-2017-sadlowski.pdf (26.01.2018).

Skwarka, M., Jargiło, M., Łasocha, M. (2012). Badanie studentów, edycja IV. *ConQuest Consulting*. Pobrano z: http://pobieranie.dlastudenta.pl/praca/pdf/BadanieStudentow.pdf (25.01.2018).

E-LEARNING IN THE GDPR CONTEXT

Keywords: GDPR, personal data, e-learning, e-learning platform

Summary. From the twenty-fifth of May 2018, the General Regulation on the Protection of Personal Data (GDPR) will become effective in the European Union. The Regulation will be a coherent tool for application in all Member States, replacing the existing legal regulations on the protection of personal data of individual EU countries. The aim of this paper is to indicate the most important changes introduced by the RODO provisions, which in the author's opinion should be taken into account in the process of identifying existing incompatibilities and gaps in the scope of personal data protection, in relation to e-learning.

Translated by Stefan Rozmus

Cytowanie

Rozmus, S. (2018). E-learning w świetle RODO. *Ekonomiczne Problemy Usług*, *2* (131/1), 303–313. DOI: 10.18276/epu.2018.131/1-30.