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

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2018.131/1-37 | strony: 379–388

Tomasz Turek
Politechnika Częstochowska
Wydział Zarządzania
Katedra Informatyki Ekonomicznej
tomasz.turek@wz.pcz.pl

Rozporządzenie o Ochronie Danych Osobowych. Aspekty organizacyjno-informatyczne w małych i średnich przedsiębiorstwach

Kody JEL: K00, K22, L38
Słowa kluczowe: RODO, GDPR, ochrona danych osobowych, system informatyczny zarządzania
Streszczenie. W artykule poruszono podstawowe aspekty wdrożenia RODO w małych i średnich przedsiębiorstwach. Duże podmioty posiadają zazwyczaj rozbudowane działy prawne i IT, które w profesjonalny sposób dostosują organizację do nadchodzących zmian. W mniejszych organizacjach RODO budzi niepokój i niepewność. Punktem wyjścia w artykule są zmiany, jakie wchodzą w życie 25 maja 2018 roku. W dalszej kolejności wskazano wymagania dla systemów informatycznych pod kątem ochrony danych osobowych. Trzecia część artykułu wskazuje na potencjalne rozwiązania, które są stosowane w tym zakresie.

Wprowadzenie

25 maja 2018 roku wchodzi w życie Rozporządzenie o Ochronie Danych Osobowych, określane skrótem RODO. Rozporządzenie to zmienia istniejącą dotychczas ustawę o ochronie danych osobowych. Przeobrażenia wynikające z RODO są przez niektórych określane jako największe zmiany w prawie po 1989 roku. Nadchodzące zmiany budzą niepokój wśród przedsiębiorców, instytucji rządowych i samorządowych, szkół, placówek służby zdrowia oraz innych podmiotów przetwarzających dane osobowe. Niepokój i niepewność są wykorzystywane przez firmy szkoleniowe, które organizują wiele konferencji i warsztatów poświęconych temu tematowi. Poruszana tematyka jest aktualna i ważna. Jednakże większość z organizowanych szkoleń dotyczy raczej

warstwy organizacyjnej i prawnej, natomiast warstwa informatyczna nie jest dostatecznie eksplorowana.

Celem artykułu jest zaprezentowanie podstawowych aspektów organizacyjnych i informatycznych, wynikających z wdrożenia RODO. Uwaga w szczególności zostanie skupiona na małych i średnich przedsiębiorstwach, gdyż te podmioty mają największe problemy, wynikające z dostosowania systemów informatycznych do nowych wymogów. Duże firmy posiadają zazwyczaj rozbudowane działy prawne oraz menedżerów IT, którzy w profesjonalny sposób zaadoptują zmiany w prawie w obszarze informatyki. Przedsiębiorstwa małe i średnie często nie są świadome, czy RODO ich dotyczy, jakie kroki powinny podjąć w warstwie organizacyjnej i informatycznej w tym aspekcie.

Rozważania zawarte w artykule bazują na tekście rozporządzenia, projekcie ustawy o ochronie danych osobowych oraz komentarzach i interpretacjach ekspertów. Ponadto wykorzystano wiedzę i doświadczenie zdobyte w projektach związanych z modernizacją i konstrukcją systemów informatycznych przedsiębiorstw pod kątem RODO.

1. Co zmienia RODO?

Jeszcze przez kilka miesięcy w polskim prawie obowiązuje ustawa z 29 sierpnia 1997 roku o ochronie danych osobowych (Ustawa, 1997). Ustawa ta jest implementacją dyrektywy 95/46/WE Parlamentu Europejskiego i Rady WE (Dyrektywa, 1995). Zawiera definicje podstawowych terminów odnoszących się do dziedziny danych osobowych, ustala zasady zbierania, gromadzenia, przechowywania i udostępniania danych osobowych. Określa zasady i warunki zgodności przetwarzania danych osobowych z prawem oraz prawa osób, których dane dotyczą. Obecnie polski i europejski system prawny jest w trakcie reformy danych osobowych. Reforma ta ma na celu ujednolicenie stopnia ochrony danych we wszystkich państwach członkowskich UE, umożliwienie swobodnego przepływu danych osobowych w ramach Unii Europejskiej oraz zapewnienie przejrzystości przepisów. Ponadto obowiązująca dyrektywa oraz ustawa mają już ponad 20 lat. Ich twórcy i ustawodawcy nie byli w stanie przewidzieć daleko idącego rozwoju technologii informacyjno-komunikacyjnych, powstawania nowych usług internetowych (Web 2.0, Web 3.0, Web 4.0), pojawiania się nowych produktów telekomunikacyjnych (w postaci innowacji produktowych czy procesowych – Budziewicz-Guźlecka, 2009, s. 520) oraz ciągle wzrastającej roli zasobów informacyjnych, w tym danych osobowych, w organizacjach wszelkiego typu – przedsiębiorstwach komercyjnych, urzędach, szkołach itp. Internet stanowi siłę napędową nowej gospodarki, stwarzając wiel szans, ale i zagrożeń, zwłaszcza w kontekście danych osobowych, które to powinny być objęte szczególną ochroną (Drab-Kurowska, 2013, s. 509).

Zmiana przepisów nie jest więc nagłą rewolucją, lecz odpowiedzią na ciągle zmieniające się warunki prowadzenia działalności gospodarczej, społecznej itp.

Nowe Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarza-

niem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – określane skrótem RODO – będzie miało zastosowanie od dnia 25 maja 2018 roku. Do tego czasu każde z państw członkowskich zobowiązane jest do zapewnienia jego skutecznego stosowania w swoim porządku prawnym poprzez przyjęcie właściwych przepisów wewnętrznych. W ramach realizacji tej kompetencji Minister Cyfryzacji przygotował projekt nowej ustawy (Ustawa, 2017) o ochronie danych osobowych oraz zmian w przepisach sektorowych. Podjęte działania legislacyjne, zgodnie z zasadami prawa Unii Europejskiej, opierały się na założeniu, że nowa ustawa o ochronie danych osobowych będzie zawierała wyłącznie przepisy, które zostały przez prawodawcę unijnego wprost przekazane do uregulowania w prawie krajowym oraz takich, w których rozporządzenie 2016/679 pozostawiło pewną swobodę regulacyjną poszczególnym państwom członkowskim (Ustawa – Ocena, 2017). Na chwilę obecną nie ma ostatecznego tekstu ustawy. Należy mieć nadzieję, że zostanie on opublikowany wraz z aktami wykonawczymi do 25 maja 2018 roku.

Skutkiem rozporządzenia będzie zakazanie stosowania rozwiązań nieprzewidzianych w rozporządzeniu i niepozostawionych wyraźnie do uregulowania w prawie krajowym. Wśród wielu zapisów RODO najważniejszymi wydają się być prawa osób, których dane dotyczą oraz obowiązki administratora. Wśród praw osób, której dane dotyczą, RODO w Rozdziale III wyróżnia: uprawnienia informacyjne, prawo dostępu do danych, prawo sprostowania danych, prawo do usunięcia danych (prawo do bycia zapomnianym), prawo do ograniczonego przetwarzania, prawo do sprzeciwu, prawo do niepodlegania automatycznym decyzjom indywidualnym. Najważniejszymi obowiązkami administratora (RODO – Rozdział IV) są: ochrona danych w fazie projektowania, domyślna ochrona danych, powierzenie przetwarzania danych, rejestrowanie czynności przetwarzania.

Zadaniem RODO jest więc znaczące rozszerzenie formuły zabezpieczenia interesów obywateli, poprzez obowiązek informowania administratora danych osobowych (tzw. ADO) o zakresie przetwarzania danych, procesach przetwarzania, okresie przetwarzania, już na etapie pozyskiwania danych. Ponadto zmianie podlegają następujące obszary:

- wprowadzenie roli inspektora ochrony danych osobowych (tzw. IOD, IODO),
- wprowadzenie rejestru czynności przetwarzania,
- zmianę statusu i roli GIODO – Generalnego Inspektora Ochrony Danych Osobowych,
- system kar.

Aktualny stan prawny wynikający z ustawy o ochronie danych osobowych nie przewiduje obligatoryjnego powoływania administratora bezpieczeństwa informacji (ABI). ABI w przedsiębiorstwie powoływany jest w sposób uznaniowy. Nowe rozporządzenie wyraźnie zmienia to podejście. Po pierwsze, w myśl RODO, miejsce admini-

stratora danych zajmuje Inspektor Ochrony Danych – tzw. IOD. Rozporządzenie wskazuje trzy sytuacje, w których powołanie IOD jest obligatoryjne:

- organ jest podmiotem administracji publicznej,
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę,
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych.

Należy zwrócić uwagę na fakt, że inspektor danych osobowych nie jest organem decyzyjnym w przedsiębiorstwie (organizacji). Jego zadaniem jest rekomendowanie określonych rozwiązań, tworzenie polityki pod kątem ochrony danych. Organem decyzyjnym pozostaje administrator danych osobowych (pracodawca). To na niego spada obowiązek ochrony danych oraz wszelka odpowiedzialność w tym zakresie. Dane kontaktowe IOD muszą być publikowane przez przedsiębiorstwo, np. na firmowej stronie WWW.

Obowiązek powoływania IOD budzi wiele kontrowersji związanych z pojęciami „główny przedmiot działalności", „duża skala" oraz „regularne i systematyczne monitorowanie". Terminy te są jednak szeroko opisywane w licznych artykułach i wyjaśniane na warsztatach i szkoleniach RODO.

Kolejnym wskazanym obszarem jest rejestr czynności przetwarzania RCP. Dotychczas w uzasadnionych przypadkach, opisanych w ustawie, przedsiębiorcy mieli obowiązek rejestracji w GIODO określonych zbiorów danych osobowych. RCP jest nowym pojęciem. Należy przez to rozumieć klasyfikowanie przetwarzania danych ze względu m.in. na: zakres przetwarzania danych, cele przetwarzania, kategorie osób, których dane dotyczą, oraz – jeśli to możliwe – środki bezpieczeństwa.

W odniesieniu do małych i średnich przedsiębiorstw istnieją różnice w interpretacji przepisów odnośnie do RCP. Niektóre publikacje wskazują, że mimo obowiązku ochrony danych osobowych, który bezwzględnie dotyczy wszystkich, prowadzenie rejestru nie jest obowiązkowe dla małych i średnich przedsiębiorstw: „Mniejsi przedsiębiorcy – wszyscy zatrudniający mniej niż 250 pracowników będą zwolnieni także z rejestrowania czynności przetwarzania danych. Wyłączenie co do prowadzenia rejestru obowiązuje jednak tylko wtedy, gdy nie są to dane osobowe wrażliwe" (Kania, 2017). Z drugiej strony art. 30 ust 5 RODO wskazuje, że rejestr czynności przetwarzania będą musieli prowadzić także:

- przedsiębiorcy lub podmioty, które przetwarzają dane osobowe osób fizycznych, w taki sposób, że może to powodować ryzyko naruszenia praw lub wolności tych osób,
- przedsiębiorcy lub podmioty przetwarzające dane w sposób niesporadyczny,
- przedsiębiorcy lub podmioty przetwarzający dane szczególne (tzw. wrażliwe).

Duże wątpliwości interpretacyjne budzą zapisy dotyczące „sporadycznego" sposobu przetwarzania, „ryzyka naruszenia praw i wolności" osób oraz „danych szczególnych". J. Kania-Stachura (2017) uważa, że „prawie każdy administrator, który jednocześnie przetwarza dane osobowe osób fizycznych w związku z prowadzoną działalnością gospodarczą, robi to zazwyczaj w sposób niesporadyczny". Ponadto wiele przypadków przetwarzania dotyczy danych szczególnych. Autorka podsumowuje swoje rozważania komentarzem: „praktycznie każdy przedsiębiorca powinien przestać zastanawiać się nad tym, czy ma obowiązek prowadzenia rejestru czynności przetwarzania i po prostu zacząć go przygotowywać".

Projekt ustawy o ochronie danych osobowych zakłada zastąpienie Generalnego Inspektora Danych Osobowych nową instytucją – Urzędem Ochrony Danych Osobowych (UODO). Wynika to z ograniczonych możliwości GIODO związanych z nakładaniem kar i egzekwowaniem przepisów związanych z ochroną i przetwarzaniem danych osobowych. UODO uzyska możliwość nakładania wysokich kar. Zgodnie z przepisami RODO mogą to być:

- 10 000 000 euro lub (dla przedsiębiorcy) do 2% światowego rocznego obrotu,
- 20 000 000 euro lub do 4% światowego rocznego obrotu w przypadku naruszeń podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9.

Reasumując powyższe rozważania z perspektywy małych i średnich przedsiębiorstw, należy zwrócić uwagę na następujący stan prawny i organizacyjny, który rozpocznie się 25 maja 2018 roku:

- wszystkie przedsiębiorstwa, organizacje i urzędy są zobowiązane do ochrony danych osobowych,
- przedsiębiorstwa powinny wprowadzić politykę bezpieczeństwa informacji; polityka ta powinna obejmować zabezpieczenia fizyczne, organizacyjne, sprzętowe i programowe,
- należy rozpatrzyć ewentualność powołania inspektora ochrony danych osobowych,
- należy przeprowadzić analizę procesów przetwarzania i w uzasadnionych przypadkach prowadzić rejestr czynności przetwarzania.

We współczesnych przedsiębiorstwach znaczna część procesów informacyjnych, w tym procesy przetwarzania danych osobowych, odbywa się w systemie informatycznym organizacji. Dlatego też przed rozwiązaniami ICT stawiane są określone wymagania.

2. RODO a systemy informatyczne w MŚP – wybrane aspekty

Podstawowym zadaniem systemów informatycznych w przedsiębiorstwach jest obsługa i wspomaganie procesów biznesowych. W zależności od specyfiki działalności gospodarczej, rodzaj i nasycenie rozwiązaniami ITC może występować w różnym stop-

niu. Mogą to być systemy klasy ERP, CRM, workflow, CAD, CAM, WMS itp. Od 25 maja 2018 roku wymagania stawiane systemom informatycznym zmieniają się. Poza merytoryczną obsługą procesów wskazane jest, aby systemy informatyczne realizowały zadania związane z:

- zapewnieniem odpowiednio wysokiego poziomu bezpieczeństwa przechowywanych danych osobowych, z uwzględnieniem ryzyka przetwarzania,
- wspomaganiem ABI/IOD w tworzeniu rejestrów czynności przetwarzania,
- wspomaganiem ABI/IOD/ADO w tworzeniu raportów i ewentualnym zgłaszaniem do GIODO/UODO powstałych incydentów związanych z naruszeniami ochrony danych osobowych,
- informowaniem osób, których dane są przetwarzane o celu, zakresie i czasie przetwarzania, a także informowaniem o sposobie kontaktu z IOD,
- wspomaganiem administratora w realizacji prawa do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osoby, która je dostarczyła administratorowi,
- realizowaniem i wspomaganiem prawa do ograniczonego przetwarzania,
- realizowaniem i wspomaganiem prawa do bycia zapomnianym.

Obowiązki te wynikają bezpośrednio z RODO, projektów ustawy o ochronie danych osobowych oraz projektów przepisów wprowadzających ustawę. W niniejszym opracowaniu uwaga poświęcona będzie najistotniejszym aspektom technologicznym: umiejscowieniu serwerowni, systemom ERP i e-handlowi. Lista aspektów, które powinny być uwzględnione, jest zdecydowanie dłuższa. Powinna obejmować: systemy monitoringu, systemy kontroli dostępu i innych rozwiązań, w których przetwarza się dane osobowe.

Zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych, które gwarantuje spójność danych, ograniczenie możliwości ich utraty, usunięcia, modyfikacji czy poufności związane jest z odpowiednio wdrożoną polityką bezpieczeństwa, obejmującą zabezpieczenia fizyczne, organizacyjne i programowe. Większość systemów informatycznych klasy ERP funkcjonuje w technologii klient–serwer. Polityka bezpieczeństwa powinna więc uwzględniać między innymi aspekt umiejscowienia serwerów i serwerowni. „Porównując koszty i uzyskiwane korzyści dotyczące wydajności, bezpieczeństwa, dostępności oraz zarządzania infrastrukturą IT, należy podjąć decyzję o optymalnie dobranych środkach, które będą wchodziły w skład systemu przetwarzania danych osobowych. Należy podjąć decyzję, czy powstanie ona w ramach własnych zasobów lokalowych i technicznych, czy należy skorzystać z usług podmiotów zewnętrznych" (Kołodziej, 2017). W przypadku własnej serwerowni do obowiązków ADO należy zapewnienie wydajności oraz odpowiedniego poziomu zabezpieczenia danych, wykonywania kopii zapasowych itp. W przypadku wykorzystania podmiotów zewnętrznych konieczne jest podpisanie z usługodawcą umowy powierzenia przetwarzania danych (podobna umowa wymagana jest w przypadku np. usług outsourcingu w obszarze rachunkowości).

Większość polskich dostawców systemów ERP i CRM (np. Macrologic Merit, Comarch Optima, Teta ERP, SAGE Symfonia ERP) oświadcza, że ich systemy są gotowe do przetwarzania danych osobowych w sposób zgodny z RODO. Wraz z wejściem w życie rozporządzenia nie będzie konieczności instalacji aktualizacji i/lub dodatków. Konieczne jest natomiast zapewnienie bezpieczeństwa przetwarzania na poziomie dostępu do systemu (identyfikatory i hasła) oraz uprawnień. Wielu administratorów systemów przypisuje użytkownikom zbyt szerokie uprawnienia, co wiąże się często z dostępem do danych osobowych. Zadaniem administratorów, ABI, ADO, IOD jest ponowna analiza polityki bezpieczeństwa w tym obszarze i odpowiednie działania ograniczające dostęp.

Nie wiadomo natomiast, w jaki sposób systemy ERP, które działają w oparciu o relacyjne bazy danych, będą realizować prawo do ograniczonego przetwarzania oraz prawo do zapomnienia. Całkowite usunięcie danych użytkownika może się bowiem wiązać z utratą spójności baz danych. Systemy ERP nie posiadają również raportów pozwalających na wyeksportowanie wszystkich danych osobowych wraz z informacją o procesach przetwarzania, na życzenie osoby, której te dane dotyczą. Przypuścić można, że prace nad tymi zadaniami są dopiero prowadzone przez producentów systemów ERP i CRM.

Wiele małych i średnich przedsiębiorstw prowadzi działalność handlową w internecie. E-handel również wymaga przemodelowania myślenia pod kątem RODO. Przede wszystkim ochronę danych osobowych należy brać pod uwagę już na etapie tworzenia serwisu WWW czy sklepu internetowego, zgodnie z regułą *privacy by design*. Jest to proaktywne podejście zakładające, że prywatność będzie chroniona nie poprzez dodatki do systemu lub nakładki przygotowane na już istniejące rozwiązania, lecz jest wbudowana w jego konstrukcję.

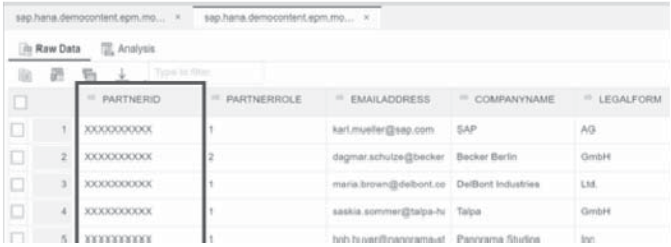
Ponieważ RODO nie wskazuje jasno, jakie technologie mają być w tym celu wykorzystywane, administratorzy muszą wykazać się dużą ostrożnością przy doborze narzędzi i usług ICT. W zasadzie każdy sklep internetowy z uwagi na wspomnianą wcześniej „niesporadyczność" przetwarzania powinien rozpatrzyć prowadzenie rejestru czynności przetwarzania. Ponadto należy zwrócić uwagę na posiadanie podstawy prawnej i zgody na przetwarzanie danych. Dotyczy to transakcji, zakładania konta, zapisu do newslettera itp. Wymaga to udowodnienia złożenia takich oświadczeń. Dotychczas stosowane przez wiele sklepów internetowych zaznaczenie *checkboxa* wydaje się być niewystarczające.

W małych i średnich przedsiębiorstwach komunikacja wewnętrzna i zewnętrzna odbywa się za pomocą standardowych usług internetowych: WWW i e-mail. Zgodnie z wytycznymi RODO zaleca się, aby komunikacja ta była szyfrowana przynajmniej na poziomie https i ssl.

3. Potencjalne rozwiązania dla systemów informatycznych w MSP

Wymagania stawiane systemom informatycznym klasy ERP po wdrożeniu RODO w większości przypadków są już spełniane przez dużych dostawców, w tym np. przez prekursora tego typu oprogramowania – firmę SAP. Można się spodziewać, że podobne rozwiązania będą wkrótce pojawiać się u innych producentów. Wśród przykładowych narzędzi należy wspomnieć SAP UI Masking oraz SAP Data Anonymization.

SAP UI Masking jest narzędziem pozwalającym na ukrywanie (maskowanie) określonych pól i kolumn w bazach danych (SAP, 2017b). Pełne dane są widoczne tylko w uzasadnionych przypadkach i w zależności od posiadanych uprawnień. W przypadku ochrony danych osobowych maskowaniu podlegać mogą pola zawierające dane wrażliwe lub dotyczące informacji pozwalających na jednoznaczne zidentyfikowanie osoby. Przykład maskowania zaprezentowano na rysunku 1.



Rysunek 1. Zastosowanie SAP UI Masking

Źródło: Aleksic (2017).

W przypadku SAP Data Anonymization określone dane osobowe lub dane wrażliwe nie są maskowane, lecz zamieniane na pseudonim. Istnieje wiele różnych sposobów tworzenia pseudonimów, np. funkcja haszująca. Przykład wykorzystania pseudonimizacji w systemie SAP zaprezentowano na rysunku 2.

Name	Birth	City	Weight	Illness
0c1a67	07-1975	Walldorf	82 kg	AIDS
df89aa	10-1975	Hamburg	110 kg	Lung Cancer
30bbe2	01-1975	Munich	70 kg	Flu

Rysunek 2. Pseudonimizacja w systemie SAP

Źródło: SAP (2017a).

W odpowiedzi na potrzeby polskiego rynku informatycznego powstają projekty, których celem jest powstanie produktu, pozwalającego na implementację go w postaci *addona* w dowolnym systemie klasy ERP. Dzięki temu systemy te byłyby zgodne z wymaganiami RODO. Podobnie jak rozwiązania SAP zapewniałyby anonimizację,

pseudonimizację, realizowały prawo do bycia zapomnianym itp. Spodziewać się można, że projekty te ujrzą światło dzienne w pierwszej połowie 2018 roku.

Podsumowanie

Wśród wielu osób prowadzących działalność gospodarczą panuje przekonanie, że zmiany związane z RODO nie dotyczą małych i średnich przedsiębiorstw. W artykule wykazano, że ochrona danych osobowych jest obowiązkiem każdego przedsiębiorcy, menedżera i pracownika. Zgodnie z wymogami rozporządzenia wiele małych i średnich przedsiębiorstw po 25 maja 2018 roku będzie musiała powołać inspektora danych osobowych i/lub rozpocząć prowadzenie rejestru czynności przetwarzania. Z uwagi na fakt, iż większość danych osobowych przetwarzanych jest w systemie informatycznym, wskazano, jakie wymagania są stawiane rozwiązaniom ITC, aby odpowiadały potrzebom RODO.

Literatura

Aleksic A. (2017). *Protect your sensitive data using SAP HANA's new dynamic data masking*. Pobrano z: https://blogs.sap.com (21.01.2018).

Budziewicz-Guźlecka, A. (2009). Nowy produkt telekomunikacyjny w aspekcie konwergencji. *Ekonomiczne Problemy Usług*, *35* (cz. 2).

Drab-Kurowska, A. (2013). Polityka konkurencji na rynku e-commerce. *Ekonomiczne Problemy Usług*, *104* (t. 1).

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Pobrano z: https://giodo.gov.pl/pl/file/2351 (21.01.2018).

http://www.wszystkoorodo.pl/rejestr-czynnosci-przetwarzania-cz-ii (21.01.2018).

Kania, R. (2017). Małe firmy też muszą zabezpieczyć dane osobowe. *Rzeczpospolita*. Pobrano z: http://www.rp.pl/Firma/303229994-Male-firmy-tez-musza-zabezpieczyc-dane-osobowe.html (21.01.2018).

Kania-Stachura, J. (2017). *Rejestr czynności przetwarzania*. Cz. 2. Pobrano z: http://www.wszystkoorodo.pl (21.01.2018).

Kołodziej, M. (2017). Własna serwerownia, kolokacja czy hosting? *ABIExpert*, *3* (4), 33–35.

Projekt z dnia 12 września 2017 r. ustawy o ochronie danych osobowych. Pobrano z: https://legislacja.rcl.gov.pl (21.01.2018).

Projekt z dnia 12 września 2017 r. ustawy o ochronie danych osobowych – ocena skutków regulacji. Pobrano z: https://legislacja.rcl.gov.pl (21.01.2018).

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). Pobrano z: https://giodo.gov.pl/pl/file/10574 (21.01.2018).

SAP Data Anonymization – FAQ (2017). Pobrano z: http://www.sap.com/data-anonymization (21.01.2018).

SAP UI Data Security (2017). Pobrano z: http://www.sap.com (21.01.2018).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz.U. 2016, poz. 922. Pobrano z: https://giodo.gov.pl/pl/file/10984 (21.01.2018).

GENERAL DATA PROTECTION REGULATION.
ORGANIZATIONAL AND IT ASPECTS IN FUNCTIONING
OF SMALL AND MEDIUM-SIZED ENTERPRISES

Keywords: GDPR, personal data protection, Business Information System

Summary. This article describes basic aspects of implementation of GDPR in small and medium-sized enterprises. Large entities usually have extensive legal and IT departments that can adapt their organization to the upcoming changes in a professional way. In smaller organizations GDPR raises anxiety and uncertainty.

The starting point in this article were legal changes, that will be introduced on May 25, 2018. Next, the requirements for IT systems in terms of personal data protection were indicated. The third part of this article indicates potential solutions that are used in GDPR.

Translated by Tomasz Turek

Cytowanie

Turek, T. (2018). Rozporządzenie o Ochronie Danych Osobowych. Aspekty organizacyjno-informatyczne w małych i średnich przedsiębiorstwach. *Ekonomiczne Problemy Usług*, *2* (131/1), 379–388. DOI10.18276/epu.2018.131/1-37.