Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 375 · 2018

Informatyka i Ekonometria 14

Radosław Pacud

Uniwersytet Ekonomiczny w Katowicach
Wydział Finansów i Ubezpieczeń
Katedra Prawa i Ubezpieczeń
radoslaw.pacud@ue.katowice.pl

PRZETWARZANIE DANYCH OSOBOWYCH W SYSTEMACH INFORMATYCZNYCH PO DNIU 25 MAJA 2018 R.

Streszczenie: Przetwarzanie danych osobowych obejmuje informacje gromadzone w systemach informatycznych, które bezpośrednio dotyczą zarówno konkretnych osób fizycznych, jak i takich, które można łatwo powiązać z konkretną osobą. Rozporządzenie, które ma bezpośredni skutek obowiązywania najpóźniej do dnia 25 maja 2018 r., będzie wymagać przed tym czasem rewizji istniejących systemów informatycznych w zakresie dotyczącym przetwarzania danych osobowych oraz uzyskania pozytywnego dostosowania do RODO. Przeprowadzone badania ankietowe w krajach UE oraz w Polsce wskazują, że duża część przedsiębiorstw uznała, że nie uzyska gotowości do kontroli przeprowadzanej przez organy nadzoru na dzień 25 maja 2018 r. Do zapewnienia zgodności przetwarzania danych w systemach informatycznych potrzebne jest wydawanie dowodów zgodności z przepisami za pomocą określonych raportów, procesów automatycznych, narzędzi informatycznych, których zastosowanie obniża ryzyko naruszenia prywatności. W artykule przeanalizowano ofertę produktów informatycznych oferowanych w tym celu na europejskim rynku producentów oprogramowania.

Słowa kluczowe: rynek oprogramowania, administrator danych osobowych, środki techniczne i organizacyjne, rozliczalność, ogólne rozporządzenie o ochronie danych osobowych.

JEL Classification: L5, O3.

Wprowadzenie – perspektywa badań informatyczno-prawnych w świetle ogólnego rozporządzenia o ochronie danych osobowych (RODO)

Celem artykułu jest rozpoznanie wymagań prawnych określonych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie

swobodnego przepływu takich danych (dalej określane jako RODO lub Rozporządzenie)[1] oraz ich wpływu na funkcjonowanie podmiotów administrujących systemami informatycznymi, tudzież rynku produktów informatycznych.

Nowe instytucje prawne w RODO oraz dokonująca się przebudowa praw podmiotowych następuje celem zwiększenia ochrony prywatności, a zwłaszcza skuteczności prawa. Zmiany te stanowią z jednej strony odpowiedź na potrzeby ochrony człowieka oraz jego pozycji prawnej w społeczeństwie informacyjnym, a z drugiej mają one sprostać wyzwaniom związanym z rozwojem technologii informatycznych i procesów globalizacji [Safjan, 2002, s. 5-6]. Powołanie organu nadzorczego w każdym kraju UE, a także rozbudowa przynależnych mu instrumentów kontrolnych i sankcyjnych prowadzi do zwiększenia regulacji przetwarzania danych osobowych w systemach informatycznych. Rozpoznanie tej regulacji oraz jej implementacja są szczególnie ważne dla adresatów RODO, którzy zostają postawieni w sytuacji koniecznej reorganizacji i dokonywania nowych wyborów ekonomicznych w zakresie stosowanych systemów informacyjnych. Chodzi tu o podmioty przetwarzające dane osobowe w systemach informatycznych, jak również uczestników rynków IT, tj. producentów i nabywców rozwiązań informatycznych. Całość kosztów dostosowania do RODO obciąża administratorów danych osobowych, którzy potrzebują wsparcia technologicznego do wykonywania nakładanych na nich obowiązków, ważnych w świetle ryzyka prawnego, tj. odpowiedzialności za ich niewykonanie. Ponoszenie takich kosztów wydaje się celowe z uwagi na zmianę otoczenia prawnego podmiotów przetwarzających danych, która jest rozpoznawana za pomocą analizy katalogu praw podmiotowych oraz obowiązków określanych przez RODO. Warto zatem spróbować odpowiedzieć na pytanie, czy ta zmiana otoczenia wymaga przebudowy systemów IT oraz aplikacji kontrolujących i wspierających rzeczywistą realizację praw podmiotów danych. Rozpatrzenie tego problemu badawczego wymaga odwołania się do wiedzy i literatury prawniczej, w zakresie europejskiego prawa ochrony danych osobowych, ale także znajomości oferty dostępnej na rynku produktów informatycznych. Zastosowana metodologia uwzględnia metodę badań rynkowych w zakresie niezbędnym do wskazania klas rozwiązań informatycznych, które pozwalają zrealizować poszczególne wymagania RODO, z kolei przeprowadzenie prawniczych badań literaturowych jest niezbędne, lecz może nie dawać satysfakcjonujących rezultatów z uwagi na krótką żywotność tego Rozporządzenia, tudzież koncentrację analiz prawnych na zagadnieniach

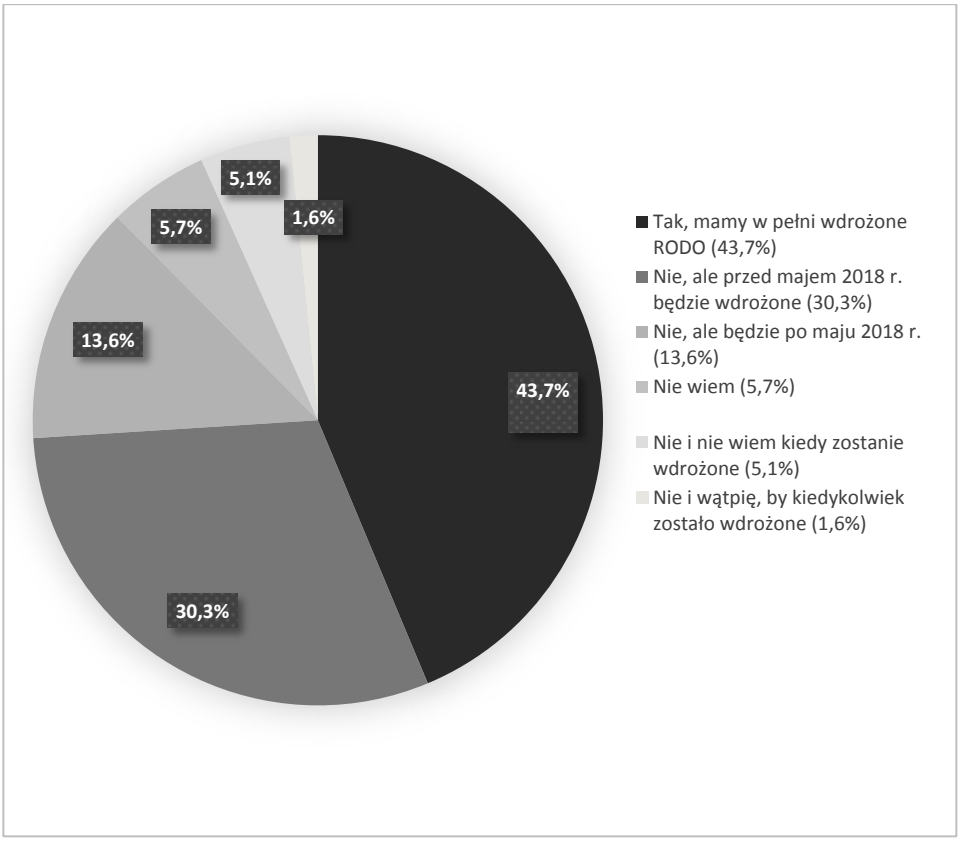
[1] W dniu 4 maja 2016 r. w Dzienniku Urzędowym UE L 119 opublikowano Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

typowo jurydycznych, a nie prakseologicznych czy też ekonomicznych. Zakłada się, że na podstawie analizy przygotowania rynku informatycznego oraz analizy prawa w kontekście podstawowych wymagań stawianych administratorom danych osobowych będzie można sformułować pewne dyrektywy przydatne do poprawy procesów *compliance* w zakresie ochrony danych osobowych, przy uwzględnieniu ocen właściwych dla podejścia *law & economics*.

Pojęcie systemu informatycznego przynależy do nauki informatyki; jest kluczowe dla rozumienia, tworzenia i zarządzania systemami informatycznymi, ale także w świetle obecnej ustawy o ochronie danych osobowych pozostaje kategorią prawną, która odnosi się do technicznego instrumentarium, za pomocą którego mogą być przetwarzane dane osobowe [Drozd, 2004]. Konieczne jest zatem spojrzenie na badane zjawisko zachowań podmiotów korzystających z systemów informatycznych przy uwzględnieniu pojęć i instrumentów wykorzystywanych w prawie oraz szeroko rozumianej informatyce, w tym informatyce ekonomicznej.

1. Przygotowania administratorów danych osobowych przed dniem 25 maja 2018 r.

Ogólne rozporządzenie o ochronie danych osobowych, uchwalone w dniu 27 kwietnia 2016 r., wywiera jednolity skutek dla podmiotów przetwarzających dane osobowe w całej Unii Europejskiej [Pacud, 2017]. Już od początku problemy z dostosowaniem systemów informatycznych do RODO zgłaszali przedsiębiorcy w najbardziej rozwiniętych krajach unijnych, które charakteryzują się wyższymi lub znacząco wyższymi od Polski poziomami PKB i rozwoju technologicznego, z czym koreluje wielkość sprzedaży produktów i siła ekonomiczna przedsiębiorstwa. Te ostatnie czynniki determinują wielkość budżetów przeznaczanych na IT oraz zdolność do przygotowania dużej organizacji do przetwarzania danych osobowych w sposób zgodny z RODO. Skalę problemów, przed jakimi stanęły polskie organizacje przetwarzające dane osobowe, sygnalizuje informacja o trudnościach napotkanych przez podobne zagraniczne podmioty. Rysunek 1 przedstawia wyniki badań ankietowych ponad 1500 organizacji z największych gospodarek unijnych, czyli Niemiec, Francji oraz Wielkiej Brytanii (przed Brexitem), przeprowadzonych w dniach 22-27 września 2017 r. [www 1]. Należałoby wnioskować, że skala problemów związanych z dostosowaniem do RODO w Polsce jest odpowiednio większa niż jest to określone na rysunku, właśnie ze wspomnianych względów ekonomicznych i technologicznych.



Rys. 1. Przygotowanie organizacji do przetwarzania danych osobowych w Wielkiej Brytanii, Francji i Niemczech. Badania ankietowe

Źródło: Na podstawie [www 1].

W lipcu 2017 r. redakcja miesięcznika „Computerworld" we współpracy z SAS Institute oraz Sygnity przeprowadziła badanie dotyczące stopnia gotowości polskich organizacji na wejście w życie RODO [www 2]. Symptomatyczny jest brak responsywności polskich menedżerów IT na wymagania RODO oraz nikły poziom przygotowań, co zapewnie powinno się już obecnie zmieniać (rys. 2). Najbardziej zaskakuje, że na rok przed wejściem RODO tak wiele organizacji nie planowało żadnych działań w zakresie dostosowania systemów informatycznych do RODO (36% respondentów).

Czy Twoja firma posiada rozwiązanie do zarządzania i dokumentowania całościowego przepływu informacji w organizacji?

Posiadamy dostosowane do RODO rozwiązanie wspierające ten aspekt Data Governance (ład danych).	11%
Jesteśmy w trakcie katalogowania całościowego przepływu informacji w organizacji w kontekście danych osobowych.	32%
Posiadamy różne silosowe rozwiązania do zarządzania danymi.	28%
Nie posiadamy tego typu rozwiązania.	18%
Trudno powiedzieć.	11%

Czy Twoja organizacja ma w planach wdrożenie lub wymianę systemu do zarządzania danymi?

Organizacja jest już w trakcie wdrożenia bądź adaptacji systemu do zarządzania danymi.	12%
Tak, w ciągu najbliższych 6 miesięcy.	4%
Tak, w ciągu najbliższych 12 miesięcy.	16%
Tak, ale później niż w ciągu roku.	7%
Nie zamierzamy wdrażać lub wymieniać systemu do zarządzania danymi w dającym się przewidzieć okresie.	36%
Trudno powiedzieć.	25%

Rys. 2. Przygotowanie organizacji do przetwarzania danych osobowych w Polsce. Badania ankietowe

Źródło: [www 2].

W najbliższych latach zostanie zweryfikowany poziom przygotowania administratorów danych do RODO w UE oraz Polsce. Kontrole organu nadzoru, który ma odpowiednie kompetencje, aby nadzorować sposoby przetwarzania danych osobowych w systemach informatycznych, będą miały na celu sprawdzenie dostosowania organizacji do wymogów prawnych od dnia 25 maja 2018 r., czyli staną się rodzajem „działania wstecz". Każde nieprzygotowanie na dzień 25 maja 2018 r. może być podstawą późniejszej oceny sposobu przetwarzania danych.

Zapowiadane kontrole administratorów danych oprócz wymagań dotyczących dostarczenia przygotowanej wcześniej dokumentacji prawnej, będą odnosiły się przede wszystkim do stanu rzeczywistego. Wymagane zatem będzie przedstawienie dowodów zgodności przetwarzania z prawem, gdyż na mocy przepisów art. 5 ust. 2 RODO, a także art. 24 RODO podmioty te będą zobowiązane w czasie kontroli oraz postępowania administracyjnego lub w przypadku ewentualnej sprawy sądowej prowadzonej z powództwa podmiotów danych wykazać, że przestrzegają przepisów RODO [Litwiński (red.), Barta, Kawecki, 2018, s. 268]. To przeniesienie ciężaru dowodowego wymaga odpowiedniego przygo-

towania systemów informatycznych, w których przetwarzane są dane, zwłaszcza przy dużej skali przetwarzania oraz dostarczania dowodów poprzez te systemy. RODO wpływa na zmianę praktyk IT, ale także na rozwój naukowy wymagający propagowania kluczowych pojęć. Dla przykładu, patrząc z perspektywy nauki zarządzania systemami IT, można się zastanawiać, jak koncepcja *governance* w organizacji, uszczegółowiana przez podejście *data governance*, prowadzi do wskazania cech jeszcze węższego zjawiska określanego mianem *privacy governance*. Działania związane z *data governance* miały na celu zapewnienie dostępu do szczegółowych danych oraz uzyskanie pełnej kontroli danych, tj. do tego, w jaki sposób trafiają do systemów IT i kto z tych systemów potem korzysta [Kotowski, b.r., s. 3]. Z kolei pod wpływem RODO większego znaczenia nabierają treści i praktyki z zakresu *privacy goverance*, które powinny zmierzać do wprowadzenia odrębnych procedur zarządzania, monitorowania danych oraz kontroli *compliance*, gdzie najistotniejsze są odpowiednio przystosowane systemy informatyczne. W ujęciu słownikowym *privacy governance* to monitorowanie ryzyka stwarzanego przez dostęp do danych, a także praktyki operatorów danych (zarządzanie informacjami) w celu zapewnienia ochrony poufności; takie zarządzanie wymaga wiedzy na temat technologii, prawa i metod statystycznych [www 3]. Celem niniejszych rozważań jest w dużym stopniu rozwiązanie problemów z zakresu *privacy governance*, pomimo braku jednolitego rozumienia pojęć z zakresu *governance* w nauce [Pawłowska, 2016, s. 17].

2. RODO jako determinanta przebudowy i rozwoju systemów informatycznych

Administratorzy danych osobowych najpóźniej od dnia 25 maja 2018 r. powinni przetwarzać je w systemach informatycznych zgodnie z RODO. Z perspektywy interesów ekonomicznych tychże administratorów, które wynikają nie tylko z celów biznesowych organizacji przetwarzających dane osobowe, ale przede wszystkim z gospodarowania zasobami organizacji w sposób ekonomiczny dostosowany do ograniczonych zasobów własnych (zwłaszcza zasobów IT), powstaje kluczowe pytanie, jak rozliczyć się z organem regulacyjnym ze stosowania RODO we własnej organizacji. Ustalenie odpowiedzi nie jest proste, gdyż przestało już obowiązywać Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, które

jasno określało, co ma administrator danych przygotować w systemie IT na wypadek ewentualnej kontroli Inspektora Ochrony Danych Osobowych.

Przedmiotem prawa określonego w RODO są dane osobowe, które stanowią kwalifikowany przez prawo rodzaj danych w rozumieniu informatycznym. Od sposobu rozumienia danych osobowych w prawie europejskim zależy, które dane uznajemy za dane osobowe, a przez to, w jaki sposób należy obchodzić się z nimi w trakcie przetwarzania w systemach informatycznych[2]. Podmiotem relewantnym dla RODO pozostaje z jednej strony osoba udostępniająca dane osobowe, która ma określone z tego tytułu uprawnienia, a z drugiej strony podmiot lub podmioty (organizacje publiczne bądź prywatne) przetwarzające dane osobowe, które nabywając prawo do przetwarzania danych osobowych, muszą wywiązać się z określonych obowiązków prawnych, a także dostosować się do istniejących zakazów.

Z uwagi na zakres zmian wprowadzanych przez RODO zachodzi konieczność odróżniania danych osobowych od pozostałych danych w systemach informatycznych, gdyż inaczej nie ma możliwości zrealizowania rozbudowanych praw osobistych podmiotów danych, szczególnie w zakresie przeprowadzenia obowiązku usuwania danych osobowych oraz realizacji prawa do zapomnienia. Dane osobowe nie mogą pozostać na zawsze w przetwarzaniu; po ustaniu bezpośredniej podstawy prawnej przetwarzania fakultatywnie mogą przejść do fazy „ograniczenia przetwarzania danych", która oznacza „przechowywanie danych osobowych w celu ograniczenia ich przyszłego przetwarzania" [RODO, art. 4, pkt. 3], a w każdym przypadku po upływie okresu retencji powinny zostać usunięte, jeżeli nie są już niezbędne do celów uzasadniających ich przetwarzanie [RODO, art. 17 ust. 1], do wywiązania się z prawnego obowiązku, do celów archiwalnych lub statystycznych [RODO art. 89 ust. 1] czy też do ustalenia dochodzenia roszczeń [RODO, art. 17 ust. 3, art. 18 ust. 2]. Po dniu 25 maja 2018 r. dane osobowe powinny być nie tylko punktem odniesienia do definiowania praw i obowiązków określających zasady przetwarzania konkretnych danych, ale również wyznacznikiem zmiany jakościowej, prowadząc do wyodrębniania danych osobowych jako obiektu w systemach informatycznych, co dopiero umoż-

[2] System informatyczny jest uznawany za skomputeryzowaną część systemu informacyjnego, która działa w sferze przetwarzania danych oraz przetwarzania informacji. Skomputeryzowany system przetwarzania danych jest rozwiązaniem technicznym, obejmującym wybrane komponenty (dane, metody i środki techniczne) [Kuraś, 2009, s. 264]. Komponentami systemu informatycznego są urządzenia i programy rozumiane jako odpowiednio uporządkowana sekwencja instrukcji, mająca na celu wykonanie określonych zadań [Urbanek, 2001, s. 168), a także procedury przetwarzania informacji oraz narzędzia programowe.

liwia zarządzanie ochroną danych osobowych (*privacy governance*). Próbując zakreślić interesującą z informatycznego punktu widzenia strukturę normatywną RODO, należy stwierdzić, iż zawiera ona w sobie pięć głównych obszarów wymagań, które rzutują na sposób przetwarzania danych w systemach informatycznych:

1. **Warunki przetwarzania danych** – dane przetwarzane w systemie informatycznym powinny mieć oznaczoną podstawę prawną, którą w razie sporu co do przypadku użycia konkretnych danych, będzie można wskazać wprost albo z polityki bezpieczeństwa, albo z systemu informatycznego. Może to być podstawa ustawowa, zgoda podmiotu danych, usprawiedliwiony interes ADO, żywotny interes podmiotu danych czy interes publiczny.
2. **Zakres przetwarzania danych** – dane przetwarzane w systemach powinny być dostosowane w swojej ilości oraz czasie przetwarzania do potrzeb i celów administratora danych osobowych. Oznacza to, że zakres jest skończony czasowy, a dane osobowe możemy podzielić na przetwarzane bez ograniczeń, ograniczone co do przetwarzania, jeżeli ustanie cel bezpośredni ich użycia oraz dane usuwane lub przeznaczone do usunięcia z systemu IT.
3. **Prawa podmiotów danych osobowych** – rozszerzenie podstawowych praw osoby, której dane są przetwarzane, tj. prawo do bycia zapomnianym, prawo do ograniczenia lub zaprzestania przetwarzania danych osobowych poza celem przetwarzania, prawo do przeniesienia danych do innego administratora danych, prawo do informacji o incydencie dotyczącym danych powierzonych (powiadomienia – 72 h).
4. **Środki techniczne i organizacyjne** – w przypadku przetwarzania danych osobowych w systemach IT trzeba wskazać, w jaki sposób będą realizowane obowiązki określone w punktach 1-3 w systemie IT oraz jakie operacje ułatwiające zarządzanie, kontrolę oraz rozliczalność z zarządzania danymi, będzie można przeprowadzić już w samym systemie IT. Realizacja obowiązków, takich jak wskazanie osób upoważnionych do danych, określanie odpowiedzialnych za stwierdzanie uchybień, rejestr czynności przetwarzania danych (prowadzenie i kontrola), może następować w samym systemie IT lub poza nim. W literaturze prawniczej za środki techniczne uznaje się zarówno rozwiązania sprzętowe, jak i programowe zapewniające ochronę przetwarzania danych [Fajgielski, 2010, s. 98]. W dalszych analizach przedmiotem zainteresowania będzie określony system komputerowy w warstwie programów, a nie całość systemu operacyjnego, który obejmuje środki autoryzacji użytkownika, kontroli dostępu czy też monitoring [Banyś, Łuczak, 2017, s. 225].

5. **Stanowienie norm zakładowych i branżowych** – doprecyzowanie norm bezpieczeństwa na poziomie zakładowym (zdefiniowanie w organizacji stosowanych technologii, w tym technologii zapewniającej automatyzację poszczególnych elementów wpływających na ochronę danych osobowych (*privacy by default*) następuje w polityce bezpieczeństwa, wiążących praktykach korporacyjnych czy też kodeksach branżowych. Do regulacji wewnętrznej pozostaje także sposób, w jaki dowodzi się przestrzegania zasad przetwarzania danych osobowych, w tym zapewnienia zdolności do potwierdzenia przestrzegania wszelkich przyjętych obowiązków w zakresie danych, szczególnie w przypadku składania roszczeń, audytów lub kontroli zewnętrznej [RODO, art. 5 ust. 2][3], ocena skutków dla ochrony danych [RODO, art. 35], określenie dokumentacji wewnętrznej.

Niewykonywanie wymienionych wyżej obowiązków jest sankcjonowane na poziomie administracyjnym [RODO, art. 83][4], cywilnoprawnym [RODO, art. 82] oraz karnym (ustawodawstwo krajowe)[5]. Analiza reguł odpowiedzialności wykracza poza zakres niniejszego opracowania.

Analizując zmiany oferty producentów oprogramowania klasy ERP, można zauważyć, że obowiązywanie RODO wywiera wpływ na tego typu systemy IT. W obszarze oprogramowania klasy ERP zachodzą zmiany związane z innym podejściem do ich obsługi, oraz zaproponowaniem nowych funkcjonalności przez producentów. Dotychczasowa koncepcja funkcjonowania tej klasy oprogramowania na podstawie procesów biznesowych uwzględniała strukturę organizacyjną podmiotu zarządzającego i rodzaj danych bądź dokumentów, ale nie odróżniała typów podmiotów – czy jest nim osoba fizyczna, która korzysta z ochrony danych osobowych, czy też osoba prawna, której przetwarzanie da-

[3] Zmiana ciężaru dowodu jest dla wielu przedsiębiorców rodzajem nadużycia siły państwa. To poważne uproszczenie, gdyż konstrukcja taka jest elementem ewolucji ochrony danych osobowych oraz stosowaniem środków prawnych, które były już znane wcześniej przy ochronie prywatności – jednostka nie musi uzasadniać ani udowadniać celów i powodów zakazu ingerencji w swą prywatność przy tajemnicy korespondencji, ochronie miru domowego czy dóbr osobistych [Sakowska-Baryła, 2015, s. 25].

[4] Odpowiedzialność administracyjna wiąże się z ryzykiem prawnym zakazu przetwarzania danych osobowych oraz ryzykiem zapłaty wysokich kar pieniężnych: a) do 10 000 000 EUR (a w przypadku przedsiębiorców do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego) w razie niewykonania określonych w RODO obowiązków administratora i podmiotu przetwarzającego, podmiotu certyfikującego oraz podmiotu monitorującego; b) do 20 000 000 EUR (a w przypadku przedsiębiorców w ramach grup naruszeń do 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego) w razie naruszenia podstawowych zasad przetwarzania, w tym warunków zgody, praw osób, których danych dotyczą, określonych w RODO, czy nieprzestrzegania nakazu orzeczonego przez organ nadzorczy.

[5] Odpowiedzialność cywilną oraz karną na gruncie obecnego ustawodawstwa oraz dotychczasowe orzecznictwo opisano w: [Banyś, Łuczak, 2017, s. 288 i n.].

nych nie podlega pod RODO. Prowadzenie monitorowalnego przetwarzania danych osobowych da się osiągnąć w pewnym stopniu na poziomie konfiguracji oraz dodatkowych narzędzi ułatwiających raportowanie danych relewantnych z punktu widzenia RODO i w formie determinowanej przez RODO. Dla przykładu, systemy Comarch ERP dostarczają już pewnych możliwości w zakresie przygotowania rejestru czynności przetwarzania danych osobowych, rejestru upoważnień przetwarzania danych osobowych, rejestru naruszeń przetwarzania danych osobowych, rejestru zgód na przetwarzanie danych osobowych, wglądu do danych osobowych, anonimizacji danych, logowania działań operatorów [www 4]. Z kolei w rozwiązaniach klasy ERP oferowanych przez Microsoft dostępny jest raport wyszukiwania osób zapewniających realizację roszczeń osób, których dotyczą dane (Dynamics 365 w rozwiązaniach Finance and Operations, Retail i Talent Core HR) [www 5]. Warto zauważyć, że w tej klasie rozwiązania również koncern SAP dodatkowo rozszerza swoje funkcjonalności w zakresie bezpieczeństwa danych (SAP Business One). W najnowszej wersji wprowadzony zostaje kreator zarządzania danymi osobowymi. Dzięki jego wykorzystaniu pojawiają się nowe możliwości w zakresie raportowania czy całkowitego usuwania danych z systemu. Ponadto w najnowszych wersjach SAP dostępna jest opcja oznaczania poszczególnych podmiotów jako osób fizycznych, dzięki czemu identyfikujemy, gdzie znajdują się dane osobowe [www 6][6]. Rynek informatyczny odpowiada zatem na zmianę otoczenia prawnego, jednak ze względu na potrzeby administratorów danych osobowych potrzebne są dodatkowe narzędzia, które wprost ułatwiają wyszukiwanie danych osobowych ze wszystkich systemów IT, a także narzędzia do zarządzania cyklem życia tych danych. Pojawiają się pomysły całościowego podejścia do zarządzania ochroną danych osobowych, które może mieć postać wydruków lub prostych plików, ale również uzyskać rozwiniętą formę zarządzania poprzez zastosowanie narzędzia informatycznego, w których identyfikowany jest postęp w zakresie realizacji celu RODO, w określonym obszarze organizacji, co oznaczono w tabeli 1 jako „Obszar *privacy governance*".

Opierając się na koncepcji Nymity Privacy Compliance Software, można zaproponować przygotowanie narzędzia informatycznego, które zbiera system ankiet lub sprawdzeń z przygotowania poszczególnych obszarów w ramach działania aktywnego, zbierającego informacje o uzyskanym poziomie *compliance*

[6] Dodane przez SAP narzędzie do wyszukiwania osób na podstawie celu przetwarzania wykorzystuje wcześniejsze możliwości oprogramowania klasy ERP. Oznaczenie oraz weryfikacja celu przetwarzania stają się możliwe poprzez skrzyżowanie struktury organizacyjnej z atrybutami procesu biznesowego i samym procesem biznesowym.

w poszczególnych datach kontrolnych [www 7]. Wydaje się, że wprost opisywane przez Nymity rozwiązanie miało ułatwiać przygotowanie do RODO przed dniem 25 maja 2018 r., lecz ze względów prawnych przestanie spełniać swoją funkcję, gdyż dostarczałoby dowodu braku dostosowania do RODO w organizacji po tej dacie. Dlatego należałoby zaproponować rozwinięcie koncepcji Nymity w ten sposób, aby raportować za pomocą podobnego narzędzia poziom skuteczności techniki IT w zakresie zapewnienia zgodności RODO. Ostatnia kolumna w tabeli 1 oznaczałaby więc jedynie poziom informatyzacji procesów zarządzania ochroną danych osobowych, co jest efektem transformacji cyfrowej poszczególnych elementów tego procesu, który opierał się na metodach tradycyjnych, lub zastosowania dodatkowych funkcjonalności i aplikacji dedykowanych lub wspierających RODO. Punktem odniesienia postępu poprawy procesów *compliance* może być więc poziom operatywności rozliczalności RODO na podstawie gromadzenia dowodów uzyskanych tradycyjnymi metodami badawczymi (ankieta, Excel, notatka, plan działania, plan sprawdzeń), które nie zapewniają zintegrowanego pomiaru efektów działań, szybkości sprawdzeń, powtarzalności, automatycznych raportów (metodologia inspektora ochrony danych osobowych). Proponowane niżej narzędzie może badać wzrost zdolności operacyjnej do rozliczenia zgodności RODO.

Tabela 1. Koncepcja karty efektywności zarządzania ochroną danych osobowych ze wskazaniem poziomu osiągniętej zdolności do rozliczenia za pomocą IT

Obszar *privacy governance* – realizacja w IT na dzień 25.12.2018	Yes (Tak)	No (Nie)	Zastosowanie technologii pomiarowej IT
1	*2*	*3*	*4*
Maintain Governance Structure (utrzymanie i koordynowanie struktury strategicznego zarządzania)	14	86	14%
Maintain Personal Data Inventory and Data Transfer (utrzymanie rejestrów danych osobowych i transferu danych)	80	20	20%
Maintain Internal Data Privacy Policy (utrzymanie wewnętrznej polityki prywatności danych)	95	5	95%
Embed Data Privacy Into Operations by Identification (osadzenie ochrony prywatności w działaniach/operacjach poprzez identyfikację danych osobowych)	25	75	25%
Maintain Training and Awareness Program (utrzymanie szkolenia i świadomości programu)	40	60	40%
Manage Information Security Risk (zarządzanie ryzykiem bezpieczeństwa informacji)	83	17	83%
Manage Third-Party Risk (zarządzanie ryzykiem realizacji praw podmiotowych)	6	94	6%
Maintain Notices (utrzymanie powiadomień)	95	5	95%

cd. tabeli 1

1	*2*	*3*	*4*
Respond to Requests and Complaints from Individuals (odpowiedzi na prośby i skargi osób fizycznych)	96	4	96%
Monitor for New Operational Practices (monitorowanie nowych praktyk operacyjnych)	9	91	9%
Maintain Data Privacy Breach Management Program (utrzymanie programu reakcji na naruszenia prywatności danych)	60	40	60%
Monitor Personal Data Handling Practices (monitorowanie procedur wymagających postępowania z danymi osobowymi)	6	94	6%
Track External Criteria (śledzenie realizacji wykonania z zewnątrz)	2	98	2%

Źródło: Na podstawie koncepcji Nymity Privacy Compliance Software [www 7]

Wskazana wyżej koncepcja karty (*scorecard*) uwzględnia z jednej strony przygotowanie do wykazania zgodności RODO za pomocą systemów IT, jak również wskazuje na uzyskany poziom transformacji cyfrowej tradycyjnych procesów *compliance*. Karta ta wspiera realizację wymagań stawianych przez zasadę *privacy by design* zakładającą, że na każdym etapie tworzenia urządzenia, systemu czy oprogramowania, w tym aplikacji oraz stron usługowych, stosowane mają być narzędzia ochrony proaktywnej i prewencyjnej, których zastosowanie zmniejsza koszt likwidacji następstw naruszeń oraz poprawek do systemu [Lubasz, 2016, s. 69-70]. W literaturze prawniczej podkreśla się, że w rezultacie zastosowania zasady *privacy by design* powinno dojść do zmniejszenia prawdopodobieństwa wystąpienia ryzyka naruszenia prywatności czy też uniknięcia następstw wystąpienia tego ryzyka [Litwiński (red.), Barta, Kawecki, 2018, s. 459]. Taką koncepcję karty łatwo wykorzystać przy rozwijaniu własnego oprogramowania, a nieco inne podejście do tego problemu można odnaleźć chociażby w produktach Microsoftu. Oferowany przez ten koncern Compliance Manager (menedżer zgodności) zapewnia użytkownikom interfejs pulpitu, w którym poszczególnym usługom przyznawane są punkty (*compliance score*) wskazujące na postępy w uzyskiwaniu zgodności[7].

[7] Menedżer zgodności to rozwiązanie działające w różnych usługach chmurowych Microsoft, które powstało, aby pomagać organizacjom spełniać założone wymogi w zakresie zgodności z przepisami, takimi jak RODO. Wykonuje ono ocenę ryzyka w czasie rzeczywistym, pokazującą poziom zgodności działań organizacji z przepisami dotyczącymi ochrony danych, także przy korzystaniu z usług chmurowych Microsoft. Przedstawia również zalecenia i szczegółowe wytyczne [www 8].

3. Oprogramowanie ułatwiające wyszukiwanie danych osobowych i realizację roszczeń informacyjnych

Prawo do informacji o danych osobowych jest realizowane już nie na wniosek uprawnionego, ale zapewniane po części *ex lege* z uwagi na obowiązek udzielenia tej informacji podmiotowi udostępniającemu dane. Pierwsza informacja przy przyjęciu danych na podstawie zgody powinna obejmować informacje o celach, podstawach prawnych oraz prawie sprzeciwu w zakresie przetwarzania informacji [RODO, motyw 50; art. 13]. Systemy informatyczne powinny ułatwiać realizację obowiązków udzielenia informacji każdej osobie fizycznej na jego wniosek, jak również wyrywkowo w czasie kontroli regulatora.

Rozporządzenie daje prawo do uzyskania nieodpłatnej kopii danych osobowych podlegających przetwarzaniu, a przy kolejnych wnioskach za rozsądną opłatą [RODO, art. 15 ust. 3]. RODO ułatwia w ten sposób realizację tzw. prawa do samookreślenia informacyjnego, w tym realizacji uprawnień korekcyjnych w zakresie usunięcia lub sprostowania informacji przetwarzanych [Sakowska-Baryła, 2015, s. 276]. Każdy administrator danych będzie musiał przekazać – na żądanie zainteresowanej osoby – informacje o niej posiadane, również w formie elektronicznej w powszechnie wykorzystywanym formacie plików. Dzięki temu łatwiej i bezpieczniej będzie przenieść dane do innego usługodawcy: banku czy towarzystwa ubezpieczeniowego, a także przekazywać dane do płatników podatków oraz składek ZUS, tudzież dane z jednej szkoły czy przedszkola do innych jednostek oświatowych. Realizacja tych obowiązków wymaga wiedzy, gdzie są zgromadzone dane osobowe konkretnych podmiotów danych. Problem pojawia się w dużych organizacjach, które przetwarzają dane osobowe w wielu systemach IT (systemach heterogenicznych), zwłaszcza gdy dane dalej migrują pomiędzy systemami IT (np. ze względu na ekonomiczną analizę danych czy archiwizację) lub też pozostają w środowiskach IT wycofanych z eksploatacji.

Do wydania informacji potrzebne jest ich wcześniejsze zebranie ze wszystkich systemów IT, w których przetwarzane są dane osobowe. W związku z tym administratorzy stają przed dylematem, czy budować kosztowne w utrzymaniu hurtownie danych osobowych, zwiększając przez to ryzyko naruszenia prywatności, czy korzystać z narzędzi identyfikujących metadane, w których systemach IT te dane się znajdują. To drugie, bardziej efektywne podejście staje się możliwe dzięki narzędziu do modelowania danych. Znany od 30 lat program Power Designer (obecnie SAP PD) umożliwia tagowanie danych oraz tworzenie tabel

pod kątem realizacji wymagań RODO[8]. Przy użyciu dodatkowej aplikacji 40Data GDPR możliwe staje się wyszukiwanie danych osobowych z kilkuset typów baz danych z wykorzystaniem metadanych gromadzonych w różnych środowiskach IT. Interfejs 40Data GDPR sięga do atrybutów wskazujących, gdzie są dane osobowe i pobiera informacje bezpośrednio z baz danych [www 9], a nie tworzy nowych silosów danych [Łabuz, 2017]. Dzięki RODO Power Designer zyskuje nowy kontekst zastosowania, a wspomniana aplikacja 40Data GDPR staje się narzędziem mającym charakter gwarantujący zgodność z RODO, zapewniając automatyczne wykonywanie operacji jako nakładka na systemy IT. Zapewne w przyszłości pojawią się też inne narzędzia na rynku, korzystające z metadanych, oraz odniesienia do oznaczeń (tagów) realizowanych na poziomie baz danych czy źródeł danych. Brakuje jednak na rynku informatycznym narzędzi do wyszukiwania danych osobowych z zapisanych dokumentów przechowanych w systemach IT, a w szczególności w poczcie mailowej. W pewnym stopniu – w zakresie odszukiwania danych z nazw plików – przydatne mogą być narzędzia do archiwizacji firmy OpenText w połączeniu z systemami ERP innych znanych producentów, względnie do anonimizacji nazw plików.

4. Oprogramowanie ułatwiające wykrywanie naruszeń ochrony danych osobowych oraz przeciwdziałające powstawaniu naruszeń

Każdorazowo w przypadku naruszenia praw podmiotów danych administrator danych osobowych ma obowiązek powiadomienia organu nadzoru oraz zawiadomienia osób, których prawa zostały naruszone. W przeciwieństwie do rozwiązań przyjętych w wielu stanach USA, w krajach UE obowiązek notyfikacji aktualizuje się niezależnie od tego, czy naruszenie dotyka dużych zbiorowości, czy też pojedynczych osób [Łabuz, 2017]. Czas notyfikacji i fakt notyfikacji mają wpływ na odpowiedzialność cywilną oraz administracyjną. Administrator danych jest zobowiązany do zgłoszenia organowi nadzorczemu naruszenia bez zbędnej zwłoki (jeżeli to wykonalne, to nie później niż 72 godziny po stwierdzeniu naruszenia)[9]. Jest to poważny problem dla polskich przedsiębiorców. Po-

[8] Trzeba odróżnić metadane, poziom modelowania tabel i zależności między nimi od procesu przechowywania konkretnych danych w tych tabelach. Power Designer pozwala na modelowanie i w tym modelu tagowanie, czyli wskazywanie pól z danymi, które mają być raportowane. Z kolei program 40Data GDPR umożliwia wyszukiwanie konkretnych danych (wystąpień) na podstawie tagów, które raz wprowadzone w procesie wdrożenia zapewniają prawidłowe raportowanie także nowych grup danych, które pojawiły się w danym systemie IT.

[9] M. Lewoszewski i A. Zdanowicz [2016] zauważają, że Europejska Rada Ochrony Danych, podczas wypełniania swoich obowiązków, opracowuje wytyczne i zalecenia, wskazując czym jest naruszenie ochrony danych oraz jak rozumieć pojęcie zbędnej zwłoki, a także identyfikuje

wstaje pytanie, czy polskie organizacje są przystosowane do wykonania obowiązków notyfikacyjnych. W Holandii według Raportu PWC na styczeń 2017 r. uznano, że tylko 76% organizacji zachowuje zgodność z RODO w zakresie przygotowania centralnej ewidencji naruszeń danych osobowych, a 72% ma przygotowane procedury komunikacyjne w odniesieniu do naruszenia danych [www 10].

Dokonując przeglądu oprogramowania ograniczającego możliwości powstawania naruszeń lub zapewniającego wykrywanie naruszeń, trzeba odwołać się do narzędzi wspomagających inwentaryzację procesów, w których przetwarzane są dane osobowe, a następnie kontrolowanie ich przebiegu. Ułatwiają to programy klasy GRC (*Governance Regulation Compliance*) oferowane przez kilka koncernów informatycznych, m.in. SAP [www 11], SAG [www 12], a także krajowych mniejszych producentów oprogramowania [www 13]. Identyfikacja procesów biznesowych w systemach IT pozwala na przeprowadzenie w nich mechanizmów kontroli, w tym monitorowania określonych kluczowych momentów w organizacji, na podstawie których może być prowadzona także kontrola ryzyka naruszenia prywatności obok kontroli innych ryzyk kluczowych dla danej organizacji (moduł *Process Control*). Dzięki temu możliwe jest szacowanie ryzyka naruszenia bezpieczeństwa danych. Oprogramowanie klasy GRC może współpracować z egzekwowaniem polityki bezpieczeństwa, np. ograniczać dostęp przy braku nadania upoważnień, kontrolować, kto ma dostęp do danych (moduł *Access Control*), informować o braku szkolenia czy innych czynnikach powiększających zarządzalne ryzyka. Moduł ten pozwala drukować raporty z dostępu do określonych rodzajów danych poszczególnych osób. Ekspozycja na ryzyko może być wyrażona w pieniądzach z uwagi na podatność organizacji na kary administracyjne oraz roszczenia pieniężne podmiotów danych, jak również w punktach, jeżeli taki sposób szacowania został zaakceptowany w organizacji[10]. W ramach narzędzia zarządzania ryzykiem przetwarzaniem danych osobowych (moduł *Risk Managment*) weryfikujemy procesy w kontekście wzrostu

okoliczności, w których administrator lub podmiot przetwarzający mają obowiązek zgłosić naruszenie danych. Takie zalecenia wskazują na urzędowy sposób wykładni pojęcia „brak zbędnej zwłoki".

[10] Z perspektywy realizacji *privacy by design* rozwiązania klasy GRC umożliwiają podejmowanie decyzji o dokonaniu nakładów (m.in. rozbudowy systemów IT oraz systemów bezpieczeństwa) celem większej mitygacji (kontroli) pojawiającego się ryzyka w oparciu o szacowane koszty braku odpowiedzi na to ryzyko. Implementacje tych rozwiązań są kluczowe dla stosowania *compliance* i rozwinęły się już przed wejściem RODO. Zapotrzebowanie w tym zakresie wzrosło po 2002 r. na fali nadużyć związanych z koncernem energetycznym ENRON, gdy w USA przyjęto prawo znane jako the Sarbanes-Oxley Act (SOX), którego celem była ochrona akcjonariuszy przed błędami popełnianymi w rachunkowości.

prawdopodobieństwa naruszenia danych osobowych[11]. Z takim oprogramowaniem, które wskazuje na zwiększanie szansy ryzyka naruszenia prywatności w określonym obszarze powinno współpracować inne, które informuje o zajściu incydentu. Przykładowo SAP Read Access Logging powiadamia o wglądzie przez konkretnego użytkownika w konkretne dane osobowe.

Innym rodzajem oprogramowania, przeciwdziałającym powstawaniu naruszeń prywatności, są narzędzia do zarządzania cyklem życia danych osobowych. Dotychczas ekonomia zasobów informatycznych zmierzała w kierunku zwiększania przestrzeni pamięci oraz liczby dysków niż usuwania informacji. RODO idzie w przeciwnym kierunku, w czym administratorów danych musi wspierać oprogramowanie. Automatyzacja w programach klasy ILM (*Information Lifecycle Managment*) oferowanych przez koncerny informatyczne SAP [www 14], IBM [www 15] czy Oracle [www 16] polega na tym, że przy wdrażaniu wprowadzone są reguły informatyczne odwołujące się do reguł prawnych (okres retencji danych), a następnie są one wpisywane w algortym, który „pilnuje", kiedy dane zostaną ograniczone w przetwarzaniu – czy to po 5 latach, czy po 15 latach.

Podsumowanie

Bezpośrednie stosowanie Rozporządzenia, które obowiązuje z bezpośrednim skutkiem od dnia 25 maja 2018 r. wymaga rewizji systemów informatycznych w zakresie dotyczącym danych osobowych, dostosowania się do nowych pojęć i definicji oraz nowego ukształtowania niektórych przesłanek przetwarzania, a także modelu komunikowania się w procesie przetwarzania wewnątrz organizacji oraz na zewnątrz z podmiotami udostępniającymi i przyjmującymi dane. RODO staje się ważnym czynnikiem wpływającym na zmiany środowisk informatycznych, a dostosowanie organizacji do nowego prawa wymaga rozbudowy już zgromadzonych lub zakupu nowych dostępnych na rynku produktów informatycznych.

Do zapewnienia zgodności przetwarzania danych w systemach informatycznych z RODO potrzebne jest wydawanie dowodów zgodności z przepisami za pomocą określonych raportów, procesów automatycznych, narzędzi informatycznych, których zastosowanie obniża ryzyko naruszenia prywatności. W artykule zbadano ofertę produktów informatycznych oferowanych w tym celu na

[11] Strukturę ścieżek postępowania określają różne prawa i obowiązki, które grupujemy i kontrolujemy różnymi regułami. Przykładem może być kontrola automatyczna, czy osoba pełniąca rolę A ma upoważnienie do przetwarzania danych typu B.

rynku producentów oprogramowania. Rozporządzenie wymaga „domyślnej ochrony danych osobowych" [RODO, motyw 78], co należy tłumaczyć jako stosowanie odpowiednich środków technicznych i organizacyjnych, które ułatwiają realizację obowiązków określonych w Rozporządzeniu. Do takich środków należą narzędzia informatyczne do inwentaryzacji zbiorów danych, pozwalające wyszukać dane osobowe, opierając się na metadanych; narzędzia do zarządzania cyklem życia danych osobowych (ILM), za pomocą których dokonuje się automatycznego przesuwania danych do fazy archiwizacyjnej i automatyczne ich usuwanie, jak również oprogramowanie klasy GRC.

Przeprowadzona analiza powinna stanowić przyczynek do rozwoju badań interdyscyplinarnych na podstawie metod z zakresu prawa, ekonomii i informatyki. Taka wieloaspektowa analiza jest ważna dla rozpatrywania problemów ekonomicznych i technologicznych dotyczących tego, jakie zasoby informatyczne pozwalają przy niskim koszcie zrealizować potrzeby określone przez normy prawne, jak również problemów prawniczych związanych z ustalaniem odpowiednich norm zakładowych w ramach polityki ochrony danych osobowych. Należy nieustannie zastanawiać sie nad stanem rozwoju techniki oraz kosztem wdrożenia środków technicznych w ramach realizacji obowiązku *privacy by design* [Litwiński (red.), Barta, Kawecki, 2018, s. 457], rozpatrywać aktualną treść obowiązkowego przystosowania systemów informatycznych do RODO, a także ewentualną odpowiedzialność za niewdrożone środki techniczne [RODO, art. 83, ust. 2 lit. D, w związku z art. 25 i 32].

Literatura

Banyś T.A.J., Łuczak J. (2017), *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych*, Presscom, Warszawa.

Drozd A. (2004), *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, LexisNexis, Warszawa, dostęp do art. 2 – lex.pl

Fajgielski P. (2010), *Kontrola i audyt przetwarzania danych osobowych*, Presscom, Wrocław.

Kotowski T. (b.r.), *Information Governance: na straży informacji* [w:] *Data Governance. Zarządzanie informacją w przedsiębiorstwie*, s. 2-4, ftp://ftp.software.ibm.com/software/pl/pdf/IBM_Data_Governance_vid.pdf (dostęp: 30.01.2019).

Kuraś M. (2009), *System informacyjny a system informatyczny – co oprócz nazwy różni te dwa obiekty?* „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie", nr 770, s. 259-275.

Litwiński P. (red.), Barta P., Kawecki M. (2018), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, C.H. Beck, Warszawa.

Lewoszewski M., Zdanowicz A. (2016), *Unia zamiesza w ochronie danych osobowych, czas się przygotować*, „Dziennik Gazeta Prawna" z 5 kwietnia (nr 65).

Lubasz D. (2016), *Europejska reforma ochrony danych osobowych. Nowe obowiązki administratorów w ogólnym rozporządzeniu o ochronie danych* [w:] E. Bielak-Jomaa, D. Lubasz (red.), *Polska i europejska reforma ochrony danych osobowych*, Wolters Kluwer, Warszawa, s. 63-85.

Łabuz J. (2017), *Bezpieczeństwo przetwarzania i zgłaszanie naruszeń dotyczących personaliów na nowych zasadach*, „Dziennik Gazeta Prawna" z 10 stycznia (nr 6).

Pacud R. (2017), *Ujednolicenie i wzmocnienie systemu ochrony danych osobowych w Unii Europejskiej* [w:] K. Głębocki, A. Bazan-Dulęda, A. Czarnecka (red.), *Unia Europejska – organizacyjne, gospodarcze, społeczne i polityczne wyzwania i perspektyw*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa, s. 59-73.

Pawłowska A. (2016), *Governance jako podejście teoretyczne – kilka kwestii spornych*, „Polityka i Społeczeństwo", nr 3(14), s. 5-17.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. Nr 100, poz. 1024.

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).

Safjan M. (2002), *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo", z. 6, s. 3-12.

Sakowska-Baryła M. (2015), *Prawo do ochrony danych osobowych*, Presscom, Wrocław.

Urbanek A. (2001), *Ilustrowany Leksykon Teleinformatyka*, Networld, Warszawa.

[www 1] https://www.proofpoint.com/sites/default/files/pfpt-uk-wp-gdpr-readiness-great-disconnect.pdf (dostęp: 31.12.2018).

[www 2] http://ascen.pl/wpcontent/uploads/2017/09/PRZYGOTOWANIA_DO_RODOW_POLSKICH_ORGANIZACJACH.pdf (dostęp: 31.12.2018).

[www 3] http://dictionary.casrai.org/Privacy_governance (dostęp: 31.12.2018).

[www 4] http://webinary.comarch.pl/systemy-comarch-erp-gotowe-na-rodo/ (dostęp: 31.12.2018).

[www 5] https://docs.microsoft.com/pl-pl/dynamics365/get-started/gdpr/ (dostęp: 31.12.2018).

[www 6] https://www.supremis.pl/rodo.html (dostęp: 31.12.2018).

[www 7] https://info.nymity.com/reporting-on-gdpr-compliance-whitepaper (dostęp: 31.12. 2018).

[www 8] https://docs.microsoft.com/pl-pl/dynamics365/get-started/gdpr/ (dostęp: 31.12. 2018).

[www 9] http://www.40data.com (dostęp: 31.12.2018).

[www 10] https://www.pwc.nl/nl/themas/assets/pdf/pwc-privacy-governance-onderzoek-2017-en.pdf (dostęp: 7.12.2018).

[www 11] https://www.sap.com/products/technology-platforms/grc.html (dostęp: 31.12. 2018).

[www 12] https://www.softwareag.com/resources/GRC-Software (dostęp: 31.12.2018).

[www 13] https://softblue.pl/softrisk/ (dostęp: 31.12.2018).

[www 14] https://www.sap.com/products/information-lifecycle-management.html (dostęp: 31.12.2018).

[www 15] https://www.ibm.com/analytics/information-lifecycle-governance (dostęp: 31.12. 2018).

[www 16] http://www.oracle.com/us/products/database/database-11g-managing-storage-wp-354099.pdf (dostęp: 31.12.2018).

PROCESSING OF PERSONAL DATA IN COMPUTER SYSTEMS AFTER MAY 25th, 2018

Summary: The processing of personal data includes all information collected in IT systems that directly concern specific individuals, as well as those that can be easily related to a specific person. The Regulation EU, which has a direct effect on the latest by 25th May, 2018, will require the revision of existing IT systems regarding the processing of personal data and a positive adjustment to the GDPR. Surveys conducted in EU countries and in Poland indicate that a large part of enterprises did not see the possibility of being prepared for Regulator as of May 25th, 2018. To ensure compliance of data processing in IT systems, it is necessary to issue evidence of compliance with regulations by means of specific reports, automated processes, an IT tools, the use of which reduces the risk of compromising privacy. The article examined the offer of IT products offered for this purpose on the European market of software producers.

Keywords: software market, personal data controller, technical and organizational measures, accountability, general data protection regulation.