PME
4/2018

PRAWO Mediów Elektronicznych

www.ksiegarnia.beck.pl
ISSN 2082-100X
Cena 65 zł (w tym 5% VAT)
C·H·BECK

PME

4/2018

Adres redakcji:

Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,
Centrum Badań Problemów Prawnych i Ekonomicznych
Komunikacji Elektronicznej
ul. Uniwersytecka 22/26, 51-145 Wrocław
e-mail: pme@beck.pl

C·H·BECK

Wydawca:

Wydawnictwo C.H. Beck
ul. Bonifraterska 17
00-203 Warszawa

tel.: 22 33 77 600
fax: 22 33 77 602
www.czasopisma.beck.pl

Nakład: 250 egz.

Spis treści

Contents

C·H·BECK

Szanowni Państwo,

z przyjemnością przedstawiam czwarty w 2018 r. numer kwartalnika naukowego Prawo Mediów Elektronicznych. Tym razem został on poświęcony w całości zagadnieniom prawa nowych technologii, w kontekście ochrony danych osobowych. W tym numerze polecamy artykuły *Gabrieli Bar* o miejscu i roli inspektora ochrony danych, *Tadeusza Białka* i *Damiana Wyrzykowskiego* o wdrażaniu RODO w bankach, *Izabeli Gil* o dochodzeniu roszczeń w aspekcie zapewnienia ochrony osób fizycznych w związku z przetwarzaniem ich danych oraz *Kajetana Wojsyka* o informatyzacji zasobów podmiotów wykonujących działalność leczniczą.

Zapraszam do lektury Prawa Mediów Elektronicznych oraz do kontaktu z nami pod adresem: pme@beck.pl

Z poważaniem
prof. dr hab. *Jacek Gołaczyński*

Inspektor ochrony danych – miejsce w organizacji, rola i zadania

dr *Gabriela Bar*[1]

Na podstawie nowych przepisów o ochronie danych osobowych, zawartych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)[2] wsparciem dla administratorów danych i podmiotów przetwarzających mają być inspektorzy ochrony danych (IOD). Ich rolą – podobnie jak poprzednio administratorów bezpieczeństwa informacji (ABI) – jest działanie na rzecz zgodnego z prawem przetwarzania danych osobowych, zarówno w jednostkach administracji publicznej, jak i w sektorze prywatnym. Celem niniejszego opracowania jest wskazanie miejsca IOD w organizacji, jego roli i zadań.

Uwagi wstępne

Koncepcja IOD nie jest w prawie europejskim nowa. Chociaż dyrektywa 95/46/WE[3] nie wprowadzała obowiązku wyznaczenia IOD, to umożliwiała (art. 18 ust. 2 oraz art. 20 ust. 2) powołanie tzw. urzędnika ds. ochrony danych osobowych (ang. *data protection official)*, a ponadto w ciągu wielu lat jej obowiązywania w niektórych państwach członkowskich rozwinęła się praktyka wyznaczania takich inspektorów.

Polska ustawa z 29.8.1997 r. o ochronie danych osobowych[4] także umożliwiała administratorom danych wyznaczenie osoby odpowiedzialnej za ochronę danych osobowych w organizacji, której funkcja została w art. 36a autonomicznie określona mianem „administratora bezpieczeństwa informacji", w skrócie ABI.

Jeszcze przed uchwaleniem i wejściem w życie RODO Grupa Robocza Art. 29 (obecnie Europejska Rada Ochrony Danych) podkreślała, że „wyznaczenie IDO może ułatwiać przestrzeganie przepisów z zakresu ochrony danych osobowych, umożliwiać budowanie przewagi konkurencyjnej na rynku oraz wdrożenie narzędzi rozliczalności (ocena skutków dla zakresie ochrony danych, przeprowadzanie lub ułatwianie audytów w zakresie bezpieczeństwa danych), a także zapewniać lepszą komunikację pomiędzy zainteresowanymi stronami (np. organami nadzoru, podmiotami danych i jednostkami biznesowymi w ramach organizacji)".

Wyznaczenie inspektora ochrony danych

Zgodnie z art. 37 ust. 1 RODO wyznaczenie inspektora ochrony danych (ang. *Data Protection Officer*, *DPO*) jest obowiązkowe w następujących przypadkach[5]:

1) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
2) 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; lub
3) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych[6] albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Ustawodawca unijny nie definiuje „organu lub podmiotu publicznego", jednak pojęcie to zostało sprecyzowane w polskiej ustawie z 10.5.2018 r. o ochronie danych osobowych[7]. W art. 9 wskazuje się, że przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora należy rozumieć:

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

Pojęcie jednostek sektora finansów publicznych definiuje art. 9 ustawy z 27.8.2009 r. o finansach publicznych[8], wskazując, że sektor ten tworzą: organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej

[1] Autorka jest radcą prawnym, partnerem zarządzającym w Szostek Bar i Partnerzy Kancelarii Prawnej.

[2] Dz.Urz. UE L119, s. 1; dalej jako: RODO.

[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz. UE L Nr 281, s. 31.

[4] T,j. Dz.U. z 2016 r. poz. 922 ze zm.

[5] Zgodnie z art. 37(4) RODO przepisy unijne bądź krajowe mogą wymuszać powołanie IOD także w innych przypadkach.

[6] Zgodnie z art. 9 RODO są to dane osobowe ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

[7] Dz.U. poz. 1000 ze zm.; dalej jako: DaneOsobU. Ustawa ta weszła w życie 25.5.2018 r.

[8] T.j. Dz.U. z 2017 r. poz. 2077 ze zm.

i ochrony prawa oraz sądy i trybunały; jednostki samorządu terytorialnego oraz ich związki; związki metropolitalne; jednostki budżetowe; samorządowe zakłady budżetowe; agencje wykonawcze; instytucje gospodarki budżetowej; państwowe fundusze celowe; Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego; Narodowy Fundusz Zdrowia; samodzielne publiczne zakłady opieki zdrowotnej; uczelnie publiczne; Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne; państwowe i samorządowe instytucje kultury; inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem jednak przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.

Status instytutu badawczego oraz NBP jako państwowych osób prawnych regulują odpowiednio: ustawa z 30.4.2010 r. o instytutach badawczych[9] i ustawa z 29.8.1997 r. o Narodowym Banku Polskim[10].

Należy mieć na uwadze, iż wykonywanie zadań w interesie publicznym lub sprawowanie władzy publicznej może być nie tylko domeną organów lub podmiotów publicznych, ale również może być realizowane przez inne osoby fizyczne i prawne podlegające prawu publicznemu lub prywatnemu, w sektorach takich jak np. transport publiczny, dostarczanie wody i energii, infrastruktura drogowa, radiofonia i telewizja, budynki użyteczności publicznej albo organy powołane dla zawodów regulowanych. Grupa Robocza Art. 29 ds. Ochrony Danych (dalej jako: GR Art. 29) w Wytycznych dotyczące inspektorów ochrony danych, WP243, przyjętych 13.12.2016 r. oraz następnie zmienionych i przyjętych 5.4.2017 r. (dalej jako: Wytyczne GR) zaleca w takich przypadkach powołanie IOD w ramach dobrych praktyk, uznając, że sytuacja osób, których dane dotyczą, może być bardzo podobna do sytuacji przetwarzania ich danych przez organy lub podmioty publiczne[11].

Zgodnie z motywem 97 RODO przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności. „Główną działalnością" będzie zatem działalność kluczowa z punktu widzenia osiągnięcia celów administratora albo podmiotu przetwarzającego.

O monitorowaniu zachowania osób, których dane dotyczą, ustawodawca unijny wspomina w motywie 24 RODO: „Aby stwierdzić, czy czynność przetwarzania można uznać za »monitorowanie zachowania« osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w Internecie, w tym także czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw". Pojęcie to – według Wytycznych GR – obejmuje wszelkie formy śledzenia i profilowania, w tym na potrzeby reklam behawioralnych, przy czym nie jest ograniczone jedynie do środowiska online i śledzenie w sieci powinno być traktowane wyłącznie jako jeden z przykładów monitorowania zachowań osób, których dane dotyczą.

GR Art. 29 definiuje pojęcie „regularne" jako: stałe albo występujące w określonych odstępach czasu przez ustalony okres; cykliczne albo powtarzające się w określonym terminie; odbywające się stale lub okresowo. Z kolei pojęcie „systematyczne" może oznaczać: występujące zgodnie z określonym systemem; zaaranżowane, zorganizowane lub metodyczne; odbywające się w ramach generalnego planu zbierania danych; przeprowadzone w ramach określonej strategii. Do przykładów podanych w Wytycznych GR zaliczają się m.in. profilowanie i ocenianie do celów oceny ryzyka (np. do celów oceny ryzyka kredytowego, ustanawiania składek ubezpieczeniowych, zapobiegania oszustwom, wykrywania zjawisk związanych z praniem pieniędzy), śledzenie lokalizacji (np. przez aplikacje mobilne); programy lojalnościowe; reklama behawioralna; monitorowanie danych dotyczących zdrowia i kondycji fizycznej za pośrednictwem urządzeń przenośnych; monitoring wizyjny[12].

Wskazówki, jak rozumieć pojęcie „dużej skali", można znaleźć w motywie 91 RODO, który stanowi, że operacje przetwarzania o dużej skali to takie, „które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko". Chodzi tu przy tym nie tylko o liczbę osób, ale także ilość danych i ich kategorii, okres i trwałość czynności przetwarzania oraz geograficzny zakres czynności przetwarzania. Jako przykład przetwarzania danych na dużą skalę Wytyczne GR wskazują: przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki, przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności lub przetwarzanie danych geolokalizacyjnych klientów w czasie rzeczywistym przez wyspecjalizowany podmiot na rzecz międzynarodowej sieci fast food do celów statystycznych[13].

W art. 37 ust. 1 lit. c) RODO nakłada na administratora obowiązek wyznaczenia IOD, gdy jego główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych z art. 9 ust. 1 RODO lub danych

[9] T.j. Dz.U. z 2018 r. poz. 736 ze zm.
[10] T.j. Dz.U. z 2017 r. poz. 1373 ze zm.
[11] Wytyczne dotyczące inspektorów ochrony danych (DPO), 16/EN WP 243 rew. 01, s. 7.
[12] Wytyczne…, s. 9–10.
[13] Wytyczne…, s. 9.

osobowych dotyczących wyroków skazujących i czynów zabronionych (art. 10 RODO).

Pojęcie „dużej skali" należy rozumieć w odniesieniu do tej przesłanki, podobnie jak zostało to opisane powyżej. Przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów i jest dokonywane przez pojedynczego lekarza lub innego pracownika służby zdrowia (por. motyw 91 RODO).

Poziom wiedzy fachowej i kwalifikacje zawodowe

Artykuł 37(5) RODO stanowi, że „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 zadań, o których mowa w art. 39". Niezbędny poziom wiedzy fachowej powinno się zaś ustalać w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe (motyw 97 RODO).

Mając na względzie powyższe przepisy oraz Wytyczne GR, należy uznać, że wiedza fachowa IOD obejmować powinna następujące elementy:

- wiedza z zakresu prawa ochrony danych osobowych: krajowego i europejskiego oraz umiejętność interpretacji przepisów prawa;
- znajomość praktyk w dziedzinie ochrony danych osobowych, w tym praktycznych aspektów wdrażania przepisów prawa w danej organizacji;
- praktyczna znajomość mechanizmów zarządzania ochroną danych (np. monitorowanie, przeprowadzanie kontroli, ocena ryzyka);
- znajomość zagadnień związanych z zastosowaniem technologii informacyjnych w przetwarzaniu danych osobowych, cyberbezpieczeństwem oraz architekturą systemów informatycznych;
- znajomość specyfiki branży, w której działa administrator lub procesor oraz wiedza o dokonywanych u danego administratora lub procesora czynnościach przetwarzania, procesach i systemach IT, w których są przetwarzane dane osobowe, oraz o kontrahentach, którym dane są powierzane do przetwarzania lub którym są przekazywane.

Choć art. 37 ust. 5 RODO nie wskazuje konkretnych kwalifikacji zawodowych, jakie należy brać pod uwagę, wyznaczając IOD, to wydaje się istotne – w świetle powyższych uwag – aby posiadał on wyższe wykształcenie, w szczególności prawnicze lub informatyczne. Przydatna jest też wiedza na temat danego sektora, a zatem w grę może wchodzić również inne wykształcenie kierunkowe.

W przypadku organów i podmiotów publicznych IOD powinien posiadać kwalifikacje w zakresie prawa i postępowania administracyjnego.

Dobrą praktyką może być uwzględnienie wytycznych dla inspektorów ochrony danych w instytucjach EU, w których zalecane jest wymaganie od IOD co najmniej siedmiu lat odpowiedniego doświadczenia, aby dana osoba mogła pełnić funkcję inspektora ochrony danych w instytucji lub organie, w których ochrona danych jest związana z podstawową ich działalnością lub które mają istotny wolumen operacji przetwarzania danych osobowych[14].

Do cech osobowych, jakimi IOD powinien się odznaczać, należą: uczciwość, etyka zawodowa, inicjatywa, dobra organizacja pracy, wytrwałość, dyskrecja, umiejętność radzenia sobie w trudnych sytuacjach, umiejętności interpersonalne: komunikacyjne, negocjacyjne czy umiejętność rozwiązywania konfliktów[15].

Wykonywanie zadań w sposób niezależny i brak konfliktu interesów

Artykuł 38 ust. 3 RODO wyznacza pewien zakres gwarancji, których celem jest umożliwianie IOD wykonywania obowiązków z odpowiednim stopniem niezależności w ramach organizacji. Administrator lub podmiot przetwarzający mają w szczególności zapewnić, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Motyw 97 RODO uzupełnia to o stwierdzenie, iż „inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny".

IOD ma wprawdzie możliwość wykonywania innych zadań i obowiązków w ramach współpracy z danym podmiotem, jednak „administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów" (art. 38 ust. 6 RODO).

W strukturze organizacyjnej IOD musi być tak umiejscowiony, aby był niezależny i aby nie dochodziło do konfliktu interesów z interesami jednostki (działu, zespołu, departamentu), w której on funkcjonuje. Rozwiązaniem zgodnym w RODO jest podleganie IOD bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego (art. 38 ust. 3 zd. ostatnie RODO). Takie rozwiązanie jest rekomendowane także przez stowarzyszenie IOD (*Network of IODs*) dla instytucji i organów UE[16]. Wytyczne te stanowią, że jedną z najlepszych praktyk pomagającą zapewnić

[14] Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 z 14.10.2010 r., https://edps.europa.eu/sites/edp/files/publication/10-10-14_IOD_standards_en.pdf (dostęp z 18.5.2018 r.).

[15] *Ibidem*.

[16] *Ibidem*.

niezależność IOD jest zapewnienie, aby raportował on bezpośrednio do szefa instytucji lub organu, który powinien być odpowiedzialny za weryfikację wykonywania obowiązków przez inspektora ochrony danych zgodnie z rozporządzeniem. Bezpośrednia podległość zapewnia najwyższemu kierownictwu wiedzę na temat porad i zaleceń IOD w ramach wypełniania przez niego zadania informowania i doradzania administratorowi lub podmiotowi przetwarzającemu. W sytuacji podjęcia przez administratora lub podmiot przetwarzający decyzji niezgodnej z przepisami RODO i zaleceniami IOD ten powinien mieć możliwość jasnego przedstawienia swojej odrębnej opinii najwyższemu kierownictwu i osobom podejmującym decyzję.

W przypadku osób prawnych, w szczególności spółek prawa handlowego, najwyższym kierownictwem administratora lub procesora będzie zarząd.

IOD nie może otrzymywać instrukcji dotyczących sposobu rozpoznania sprawy, środków, jakie mają zostać podjęte, celu, jaki powinien zostać osiągnięty, czy też faktu, czy należy skontaktować się z organem nadzorczym. IOD nie może być obligowany do przyjęcia określonego stanowiska w sprawie z zakresu prawa ochrony danych, np. określonej wykładni przepisów.

Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny, co oznacza, że IOD nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Stanowiska niekompatybilne z funkcją IOD (powodujące konflikt interesów) to m.in.: stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), jak również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych[17].

Zadania IOD i zapewnienie możliwości ich realizacji

Zgodnie z art. 39 RODO do zadań IOD należą:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o ich obowiązkach wynikających z przepisów o ochronie danych osobowych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania obowiązujących przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4) współpraca z organem nadzorczym oraz wypełnianie funkcji punktu kontaktowego dla organu nadzorczego.

IOD powinien – zgodnie z opracowanym planem swoich działań – informować, doradzać i rekomendować określone działania administratorowi lub procesorowi.

Artykuł 39 ust. 1 lit. a RODO nie tylko dotyczy obowiązków ochrony danych określonych przepisami RODO, lecz także wskazuje, iż obowiązki te mogą wynikać z przepisów odrębnych ustaw. W rezultacie w sytuacji, gdy organizacja funkcjonuje w sektorze dodatkowo regulowanym (np. banki), to należy uwzględnić odrębne przepisy regulujące ochronę danych osobowych i bezpieczeństwo informacji w ogóle.

W ramach monitorowania przestrzegania przepisów IOD powinien m.in.:

- zbierać informacje w celu identyfikacji procesów przetwarzania;
- analizować i sprawdzać zgodność tego przetwarzania z RODO i innymi odnośnymi przepisami prawa;
- przeprowadzać kontrole w zakresie prawidłowości przetwarzania danych w organizacji;
- rekomendować określone działania;
- przeprowadzać szkolenia personelu uczestniczącego w operacjach przetwarzania.

Wprawdzie do obowiązków administratora, a nie IOD, należy przeprowadzanie w określonych przypadkach oceny skutków dla ochrony danych, jednak art. 35 ust. 2 RODO nakłada na administratora obowiązek konsultowania się z IOD przy jej dokonywaniu. Natomiast w art. 39 ust. 1 lit. c) RODO określono obowiązek IOD udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych zgodnie z art. 35 RODO. Wobec tego administrator powinien konsultować z IOD co najmniej:

- fakt, czy należy przeprowadzić ocenę skutków dla ochrony danych;
- metodologię przeprowadzenia oceny skutków dla ochrony danych;
- fakt, czy należy przeprowadzić wewnętrzną ocenę skutków dla ochrony danych czy też zlecić ją podmiotowi zewnętrznemu;
- zastosowania konkretnych zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
- prawidłowość przeprowadzonej oceny skutków dla ochrony danych i zgodność jej wyników z wymogami ochrony danych.

[17] Wytyczne..., s. 17.

IOD ma pełnić funkcję punktu kontaktowego, by umożliwić organowi nadzorczemu dostęp do dokumentów i informacji w celu realizacji zadań, o których mowa w art. 57 RODO, jak również wykonywania uprawnień w zakresie prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń oraz uprawnień doradczych, zgodnie z art. 58 RODO.

Wprawdzie IOD związany jest tajemnicą i poufnością dotyczącą wykonywania zadań IOD, ale zakaz ten nie wyłącza możliwości kontaktowania się IOD z organem nadzoru w celu uzyskania porady co do właściwej ścieżki postępowania w danych okolicznościach (art. 39 ust. 1 lit. e) RODO).

Należy zwrócić uwagę, że art. 39 ust. 1 RODO w wersji angielskiej stanowi, że IOD „*shall have »at least« the following tasks*" („do obowiązków IOD należy co najmniej"). W związku z tym zakres obowiązków IOD może być szerszy lub bardziej szczegółowo opisany, niż ma to miejsce w art. 39 ust. 1 RODO. W szczególności należy uznać za praktyczne rozwiązanie, aby IOD:

- stanowił punkt kontaktowy dla podmiotów danych – w sprawach związanych z realizacją ich praw;
- prowadził rejestr czynności przetwarzania lub rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora (art. 30 ust. 1 i 2 RODO);
- prowadził rejestr naruszeń i dokumentację wymaganą art. 33 ust. 5 RODO.

W związku z powyższymi zadaniami administrator lub procesor powinni zapewnić udział IOD we wszystkich zagadnieniach związanych z ochroną danych osobowych (art. 38 RODO), np. poprzez:

- udział w spotkaniach kadry kierowniczej (wyższego i średniego szczebla),
- udział w procesach decyzyjnych – otrzymywanie istotnych informacji w wyprzedzeniem,
- uwzględnianie opinii IOD na etapie projektowania procesów i w toku przetwarzania danych,
- konsultacje z IOD w przypadku stwierdzenia naruszenia albo innego incydentu związanego z danymi osobowymi.

Zespół wspierający IOD

W zależności od rozmiaru i struktury organizacji przydatne może być powołanie zespołu inspektora ochrony danych[18]. Wskazanie pozytywnego katalogu wszystkich możliwych zadań nakładanych na IOD oraz kierowany przez niego zespół nie jest możliwe, gdyż w dużej mierze zależeć on będzie od decyzji administratora lub procesora. Zadania te można jednak podzielić na trzy grupy:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o konkretnych obowiązkach spoczywających na nich na podstawie RODO i in. przepisów regulujących kwestie bezpieczeństwa przetwarzania danych osobowych;
2) merytoryczne wsparcie administratora danych, podmiotu przetwarzającego oraz pracowników w podejmowaniu działań zmierzających do zapewnienia zgodnego z prawem przetwarzania danych;
3) egzekwowanie przestrzegania zasad ochrony danych.

W przepisach prawa lub wytycznych GR Art. 29 nie zostały wskazane żadne ograniczenia co do tego, w jakim zakresie IOD może delegować swoje kompetencje na pracowników zespołu. Nie ulega jednak wątpliwości, iż w stosunkach zewnętrznych związanych z pełnioną przez IOD funkcją, zawsze powinien on występować osobiście. Podobnie rzecz ma się z podejmowaniem decyzji, co do przeprowadzenia kontroli w kwestii zgodności z RODO przetwarzania danych osobowych oraz wyrażania opinii co do działań rekomendowanych administratorowi. Szczegółowy podział kompetencji i obowiązków powinien określać regulamin zespołu IOD lub inne wewnętrzne regulacje w danej organizacji.

Zawiadomienie o wyznaczeniu IOD i publikowanie jego danych

Przepis art. 10 DaneOsobU wprowadza obowiązek zawiadomienia o wyznaczeniu IOD Prezesa Urzędu Ochrony Danych Osobowych, który prowadzi wewnętrzną ewidencję zawiadomień. Obowiązek ten spoczywa na podmiocie wyznaczającym: administratorze lub procesorze i powinien być spełniony w terminie 14 dni od dnia wyznaczenia IOD. Zawiadomienie obejmuje: imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora. O każdej zmianie danych należy zawiadomić w terminie 14 dni od dnia zaistnienia zmiany.

Zawiadomienia można dokonać wyłącznie w postaci elektronicznej – wymaga ono jednak opatrzenia kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Oprócz konieczności zawiadomienia organu administrator i procesor są zobowiązani opublikować na swojej stronie internetowej – niezwłocznie po wyznaczeniu inspektora – następujące dane IOD: imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora (art. 11 DaneOsobU). Jeśli dany podmiot nie prowadzi własnej strony internetowej, to takiej publikacji powinien dokonać w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Rozwiązanie to wydaje się niezgodne z RODO. Artykuł 37 ust. 7 RODO nie wymaga bowiem publikowania imienia i nazwiska inspektora, a jedynie podania jego danych kontaktowych, czyli np. adresu korespondencyjnego, numeru telefonu kontaktowego lub dedykowanego adresu e-mail. Zgodnie

[18] Wytyczne…, s. 15.

z Wytycznymi GR wskazanie dodatkowych informacji może być dobrą praktyką, ale decyzja o tym, czy w określonych okolicznościach udostępnienie tych danych może być konieczne lub pomocne, zależeć powinno od administratora lub podmiotu przetwarzającego i IOD[19].

Podsumowanie

Należy pamiętać, iż wyznaczenie IOD jest jednym z wielu działań, które organizacja powinna lub może podjąć, aby funkcjonować w zgodzie z przepisami z zakresu ochrony danych osobowych. Pomimo istotnej roli IOD i wagi wypełnianych przez niego zadań IOD nie jest osobiście odpowiedzialny za przestrzeganie tych przepisów przez podmiot, w ramach struktury którego działa. W każdym wypadku to administrator lub podmiot przetwarzający jest zobowiązany zapewnić i być w stanie wykazać, że przetwarzanie odbywa się zgodnie z RODO lub innymi odnośnymi przepisami prawa (art. 24 ust. 1 RODO).

[19] Wytyczne…, s. 14.

Słowa kluczowe: inspektor ochrony danych, IOD, DPO, RODO, GDPR, dane osobowe, przetwarzanie danych osobowych, podmioty danych, naruszenia danych osobowych, niezależność inspektora ochrony danych, konflikt interesów, zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych.

Data Protection Supervisor – place in the organization, role and duties

Based on new regulations on personal data protection included in the regulation of the European Parliament and of the Council 2016/679 of 27.4.2016, in the matter of protection of natural persons in regard to processing of personal data and in the matter of free movement of such data and repealing the directive 95/46/EC (general data protection regulation), the support for data administrators and entities processing data are going to be data protection supervisors (DPS). The role of those supervisors – just like before with information security administrators (ISA) – is to act in the interest of processing data protection in accordance with law, both in public administration units, and in the private sector. The aim of the present study is to show the place of DPS in an organization, their roles and duties.

Keywords: data protection supervisor, DPS, GDPR, personal data, processing of personal data, subjects of data, violating personal data, independence of data protection supervisor, conflict of interest, notifying the President of Personal Data Protection Office.

Wdrażanie RODO w bankach na przykładzie „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe”[1]

dr *Tadeusz Białek*[2]
Damian Wyrzykowski[3]

Celem niniejszego opracowania jest prezentacja opracowanego przez Związek Banków Polskich projektu „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe” (dalej jako: Kodeks) jako przykładu działań wdrażających rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)[4] w polskim sektorze bankowym oraz jego podmiotach. Aby umożliwić bezpośrednie odniesienie ww. zagadnienia do kontekstu legislacyjnego w postaci RODO, omówienie treści projektu Kodeksu zostanie poprzedzone ogólną charakterystyką instytucji kodeksu postępowania (*code of conduct*) na gruncie przepisów tego rozporządzenia.

Uwagi wstępne

Z dniem 25.5.2018 r. rozpoczęło się stosowanie RODO. Zakres oraz charakter zmian przewidzianych przez ten akt prawny jest na gruncie literatury często określany jako rewolucyjny[5], zwłaszcza w odniesieniu do zadań oraz obowiązków administratorów danych osobowych[6]. W tym też kontekście podnosi się, iż w ramach wprowadzanych przepisów na administratorów danych osobowych przeniesiony zostaje znacznie większy ciężar odpowiedzialności za przestrzeganie zasad i obowiązków wynikających z RODO[7].

Banki – jako podmioty, na których funkcjonowanie przepisy RODO wpływają w znaczący, wszechstronny sposób – już w momencie wejścia w życie RODO, tj. w maju 2016 r., prowadziły działania mające na celu pełne oraz skuteczne dostosowanie swojej działalności do nowych wymogów stawianych przez ten akt prawny. W szczególności należy zwrócić uwagę, iż Związek Banków Polskich – jako izba gospodarcza w rozumieniu ustawy z 30.5.1989 r. o izbach gospodarczych[8] – rozpoczął działania mające na celu informowanie podmiotów polskiego sektora bankowego o zmianach zakładanych przez RODO jeszcze przed wejściem jego przepisów w życie[9]. Mając więc na względzie kluczowe znaczenie dwuletniego okresu dostosowawczego do RODO, który rozpoczął się wraz z wejściem przedmiotowego rozporządzenia w życie[10], banki-członkowie Związku Banków Polskich przyjęły, że jednym z najistotniejszych aspektów pełnego dostosowania polskiego sektora bankowego do wymogów RODO jest opracowanie Kodeksu sektorowego mającego stanowić kodeks postępowania w rozumieniu art. 40 RODO.

Kodeks postępowania (*code of conduct*) jako instytucja przewidziana na gruncie RODO

W art. 40 RODO uregulowano instytucję kodeksów postępowania, która – choć była już znana oraz stosowana na dotychczasowym gruncie prawa ochrony danych[11]

[1] Niniejszy artykuł opiera się na brzmieniu projektu „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe” w wersji z 10.1.2018 r., która na chwilę pisania niniejszego artykułu jest jego najbardziej aktualną wersją. Autorzy zastrzegają możliwość zmiany brzmienia dotychczasowego projektu „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe” oraz zmiany stanu prawnego po dacie przekazania niniejszego artykułu redakcji.

[2] Radca prawny, doktor nauk prawnych, Dyrektor Zespołu Prawno-Legislacyjnego Związku Banków Polskich.

[3] Aplikant radcowski, doktorant na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego, prawnik w Zespole Prawno-Legislacyjnym Związku Banków Polskich.

[4] Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

[5] *M. Kawecki*, Prawo ochrony danych osobowych jako nowa dziedzina prawa, EPS 2017, Nr 5, s. 4.

[6] *P. Kozik*, Zakres swobody regulacyjnej państw członkowskich przy wdrażaniu ogólnego rozporządzenia o ochronie danych osobowych do prawa krajowego, EPS 2017, Nr 5, s. 17.

[7] *E. Bielak-Jomaa*, Ogólne rozporządzenie o ochronie danych. Rewolucja w ochronie danych?, dodatek MoP 2017, Nr 20, s. 3.

[8] T.j. Dz.U. z 2017 r. poz. 1218 ze zm.

[9] Zob. np. informację o zorganizowanej przez Związek Banków Polskich konferencji „Nowa regulacja przetwarzania danych osobowych – General Data Protection Regulation – skutki w sektorze finansowym”, która odbyła się 10.3.2016 r.: https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/marzec/nowa-regulacja-przetwarzania-danych-osobowych-general-data-protection-regulation-skutki-w-sektorze-finansowym (dostęp z 26.4.2018 r.).

[10] *E. Bielak-Jomaa*, Ogólne rozporządzenie…, s. 3.

[11] *P. Litwiński* (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Warszawa 2018, s. 596; *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018, s. 821.

– wraz z przyjęciem RODO zyskuje nowy wymiar m.in. poprzez jej dalej idące sformalizowanie oraz wprowadzenie wielu domniemań prawnych łączących się z kodeksami postępowania[12]. W szczególności podkreśla się, że na gruncie RODO instytucja kodeksów postępowania zyskuje na znaczeniu ze względu na zwiększenie możliwości zastosowania mechanizmów wykazania zgodności prowadzonych operacji przetwarzania danych z obowiązującymi przepisami[13].

Zgodnie z art. 40 ust. 1 RODO państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja Europejska zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu RODO. Jak wskazuje przy tym przywołany przepis, kodeksy postępowania powinny być sporządzane z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania, jak również szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. W tym też kontekście podkreśla się, iż kodeksy postępowania mają charakter uregulowań sektorowych[14], stanowiąc instrument samoregulacyjny wspomagający oraz usprawniający proces wdrożenia przepisów RODO i krajowego ustawodawstwa przyjętego na podstawie RODO[15]. Stosowanie kodeksów postępowań ma więc istotne znaczenie dla sposobu realizacji zasad oraz obowiązków wynikających z RODO, jako że kodeksy postępowania wyjaśniają oraz dostosowują tak określone wymogi do konkretnych sektorów i związanej z nimi specyfiki[16]. W tym miejscu można również przywołać treść motywu 98 RODO, w myśl którego sporządzanie kodeksów postępowania ma ułatwiać skuteczne stosowanie RODO „z uwzględnieniem szczególnych cech przetwarzania prowadzonego w niektórych sektorach i szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw", przy czym w kodeksach postępowania „można w szczególności dopasować obowiązki administratorów i podmiotów przetwarzających do ryzyka naruszenia praw lub wolności osób fizycznych, jakie może powodować przetwarzanie". W powyższym kontekście zwraca się więc również uwagę na korzyści płynące ze stosowania kodeksów postępowania, nie ograniczając ich przy tym wyłącznie do sfery zwiększenia poziomu przestrzegania wymogów RODO przy przetwarzaniu danych[17]. W tym też względzie wskazuje się, iż stosowanie kodeksów postępowań jest korzystne zarówno dla osób, których dane dotyczą, jak i samych administratorów oraz podmiotów przetwarzających[18].

Co ważne, choć kodeksy postępowania zalicza się do kategorii instrumentów prawa miękkiego (*soft law*)[19], na gruncie RODO pełnią one znaczącą funkcję niosącą ze sobą wiele istotnych implikacji. Kodeksów postępowania w rozumieniu art. 40 RODO nie należy więc traktować jako instrumentów o wyłącznie informacyjnym czy też wizerunkowym charakterze[20]. W szczególności zwraca się uwagę, że poprzez przyjęcie kodeksu postępowania członkowie określonego zrzeszenia (zob. uwagi niżej) zobowiązują się dostosować swoje działania oraz stosować regulacje zawarte w kodeksie, podlegając konsekwencjom ich ewentualnego naruszenia[21]. W tym też kontekście należy pamiętać, iż przepisy RODO przewidują stosowanie mechanizmów kontroli przestrzegania postanowień kodeksów postępowań[22].

Zgodnie z art. 40 ust. 2 RODO zrzeszenia oraz inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające mogą opracowywać lub zmieniać kodeksy postępowania lub rozszerzać ich zakres w celu doprecyzowania zastosowania RODO. Na gruncie przywołanego przepisu wskazuje się więc, iż RODO w sposób wyraźny określa dwie kategorie podmiotów mogących wystąpić z inicjatywą dotyczącą kodeksu postępowania, implikując tym samym brak uprawnienia do tworzenia kodeksu postępowania przez indywidualnego administratora[23]. Jednocześnie na gruncie RODO możliwe jest sporządzanie kodeksów postępowania przez organy oraz podmioty publiczne[24]. Podnosi się przy tym również, że przepisy RODO nie definiują pojęcia „zrzeszenia", przez co może być ono rozumiane w różny sposób – na gruncie polskiego prawa przyjmuje się, iż przykładem zrzeszenia, o którym mowa w art. 40 RODO, jest izba gospodarcza[25] (a więc np. Związek Banków Polskich). W tym też względzie na gruncie RODO katalog zrzeszeń mogących wystąpić z inicjatywą dotyczącą kodeksu postępowania jest szeroki i zależny od ustawodawstwa poszczególnych państw członkowskich UE[26].

W art. 40 ust. 2 RODO określono również zakres przedmiotowy kodeksów postępowania, przy czym wyliczenie zawarte w art. 40 ust. 2 lit. a)–k) RODO ma wyłącznie przykładowy charakter, skutkując możliwością uregulowania w kodeksach postępowania również innych kwestii dotyczących stosowania RODO[27]. Zgodnie z przywołanym

[12] *P. Litwiński* (red.), Rozporządzenie…, s. 596–597.
[13] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 821–822.
[14] *P. Litwiński* (red.), Rozporządzenie…, s. 597.
[15] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 819.
[16] *Ibidem.*
[17] *Ibidem.*
[18] *Ibidem.*
[19] *Ibidem.*
[20] *Ibidem.*
[21] *Ibidem.*
[22] *P. Litwiński* (red.), Rozporządzenie…, s. 599; *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 827.
[23] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 824.
[24] *P. Litwiński* (red.), Rozporządzenie…, s. 598.
[25] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 824.
[26] *Ibidem.*
[27] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 825; *P. Litwiński* (red.), Rozporządzenie…, s. 598.

przepisem kodeksy postępowania mogą doprecyzować zastosowanie RODO m.in. w odniesieniu do: rzetelnego i przejrzystego przetwarzania (art. 40 ust. 2 lit. a); prawnie uzasadnionych interesów realizowanych przez administratorów w określonych kontekstach (art. 40 ust. 2 lit. b); zbierania danych osobowych (art. 40 ust. 2 lit. c); pseudonimizacji danych osobowych (art. 40 ust. 2 lit. d); informowania opinii publicznej i osób, których dane dotyczą (art. 40 ust. 2 lit. e); wykonywania przez osoby, których dane dotyczą, przysługujących im praw (art. 40 ust. 2 lit. f); informowania i ochrony dzieci oraz sposobu pozyskiwania zgody osoby sprawującej władzę rodzicielską lub opiekę nad dzieckiem (art. 40 ust. 2 lit. g); środków i procedur, o których mowa w art. 24 i 25 RODO, oraz środków zapewniających bezpieczeństwo przetwarzania, o których mowa w art. 32 RODO (art. 40 ust. 2 lit. h); zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą (art. 40 ust. 2 lit. i); przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych (art. 40 ust. 2 lit. j); postępowań pozasądowych oraz innych trybów rozstrzygania sporów w celu rozstrzygania sporów między administratorami a osobami, których dane dotyczą, w zakresie przetwarzania, bez uszczerbku dla praw osób, których dane dotyczą, na mocy art. 77 i 79 RODO (art. 40 ust. 2 lit. k).

W kontekście zakresu przedmiotowego kodeksu postępowania podnosi się, iż jego regulacje powinny obejmować w pierwszej kolejności zagadnienia dotyczące specyfiki określonego sektora oraz jej wpływu na ogólne zasady ochrony danych[28]. Co istotne, postanowienia kodeksu postępowania muszą być zgodne z obowiązującymi przepisami i nie mogą prowadzić do obniżenia poziomu ochrony danych przewidzianego przez RODO[29].

Zgodnie z art. 40 ust. 5 RODO zrzeszenia oraz inne podmioty chcące opracować kodeks postępowania lub zmienić lub rozszerzyć zakres kodeksu już obowiązującego są zobowiązane przedłożyć projekt kodeksu, zmiany lub rozszerzenia organowi nadzorczemu właściwemu na podstawie art. 55 RODO. Organ nadzorczy przeprowadza ocenę, a następnie wydaje opinię o zgodności ww. projektu z RODO i – jeżeli uzna, że stanowi on odpowiednie zabezpieczenia – zatwierdza taki projekt kodeksu, zmiany lub rozszerzenia. Na gruncie art. 40 ust. 6 RODO zatwierdzony projekt kodeksu, zmiany lub rozszerzenia jest następnie rejestrowany oraz publikowany przez organ nadzorczy – jeśli nie dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich UE. Jeżeli bowiem projekt kodeksu postępowania dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich, zastosowanie znajduje procedura określona w art. 40 ust. 7–11 RODO, przewidująca uwzględnienie mechanizmu spójności, o którym mowa w art. 63 RODO[30].

„Kodeks dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe" jako kodeks postępowania (*code of conduct*) dla polskiego sektora bankowego

Mając na względzie wyżej zarysowaną charakterystykę oraz zalety instytucji kodeksów postępowania na gruncie RODO, jak również wychodząc z założenia, iż opracowanie oraz przyjęcie kodeksu postępowania pozwala na lepsze przygotowanie danego sektora do wykazania zgodności procesów przetwarzania danych z przepisami RODO[31], wraz z wejściem RODO w życie w maju 2016 r. Związek Banków Polskich rozpoczął intensywne prace nad projektem stosownego dokumentu, który miałby stanowić kodeks postępowania dla polskiego sektora bankowego. Jednym z najważniejszych założeń przyjętych przez Związek Banków Polskich było przy tym, aby opracowywanie Kodeksu przedstawiało interdyscyplinarny charakter umożliwiający wszechstronne spojrzenie na procesy przetwarzania danych dokonywane przez banki oraz rejestry kredytowe. W tym też względzie Związek Banków Polskich dołożył znacznych starań, aby przedstawiciele banków oraz rejestrów kredytowych biorący udział w bezpośrednim projektowaniu oraz konsultacji Kodeksu reprezentowali wszystkie obszary kluczowe z punktu widzenia omawianego zagadnienia.

Co istotne, mając nieustannie na uwadze, iż kodeks postępowania ma służyć nie tylko administratorom oraz podmiotom przetwarzającym, lecz również – w takim samym stopniu – osobom, których dane dotyczą[32], Związek Banków Polskich projektując Kodeks, przywiązywał szczególną wagę do sposobu formułowania jego treści. Jeżeli bowiem stosowanie kodeksów postępowania ma na celu m.in. podnoszenie poziomu świadomości ochrony danych oraz budowanie zaufania do jakości procesów przetwarzania danych[33], Związek Banków Polskich uznał za niezbędne, aby projektowany Kodeks był przejrzysty oraz zrozumiały dla jak najszerszego grona odbiorców. W tym też względzie przyjęto, iż choć język Kodeksu ma odzwierciedlać terminologię RODO, postanowienia Kodeksu powinny być formułowane w sposób zrozumiały nie tylko dla osób profesjonalnie zajmujących się problematyką prawa ochrony danych osobowych, lecz także dla osób, które w bankach zajmują się obsługą Klientów oraz samych Klientów banku lub rejestru kredytowego.

[28] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 825–826.
[29] *Ibidem.*
[30] *P. Litwiński* (red.), Rozporządzenie…, s. 601.
[31] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 821.
[32] *Ibidem.*
[33] *Ibidem.*

Dla Związku Banków Polskich równie istotne było także położenie nacisku na aspekt praktyczny Kodeksu. Stąd też Kodeks tylko w niezbędny sposób odnosi się wprost do postanowień RODO, starając się przełożyć dyspozycje RODO na praktyczne opisy stosowania określonych instytucji RODO w praktyce bankowej (np. prawo do bycia zapomnianym, prawo do przenoszenia danych, obowiązek informacyjny).

Efektem powyższych starań było sfinalizowanie na forum Związku Banków Polskich – po blisko półtora roku prac – projektu Kodeksu z końcem grudnia 2017 r. Ogólne założenia projektu Kodeksu zostały następnie zaprezentowane publicznie podczas zorganizowanych przez Generalnego Inspektora Ochrony Danych Osobowych 11.1.2018 r. warsztatów „Kodeksy postępowania w świetle RODO"[34].

Główne założenia „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe"

Główne założenia Kodeksu zostały w bezpośredni sposób sformułowane we wprowadzeniu do Kodeksu (dalej jako: Wprowadzenie), które zawiera postanowienia opisujące zakres podmiotowy oraz przedmiotowy Kodeksu, jak również wskazuje ogólne cele, które mają zostać osiągnięte przez przyjęcie oraz stosowanie Kodeksu.

Zgodnie z przyjętymi założeniami Kodeks stanowi zbiór zasad postępowania w zakresie ochrony danych osobowych w polskim sektorze bankowym (ust. 1 Wprowadzenia), będąc doprecyzowaniem zasad przetwarzania i ochrony danych osobowych określonych w RODO z uwzględnieniem specyfiki sektora bankowego (ust. 2 Wprowadzenia). W tym też miejscu warto zwrócić uwagę, że twórcy Kodeksu w sposób bezpośredni zawarli odniesienie do pojęcia „specyfiki sektora bankowego", co stanowi wyraźne nawiązanie do wskazanej na gruncie motywu 98 RODO i art. 40 ust. 1 RODO charakterystyki kodeksów postępowania jako uregulowań sektorowych[35], dostosowujących wymogi RODO do specyfiki konkretnych sektorów[36]. Ponadto, w celu uniknięcia jakichkolwiek wątpliwości odnośnie do charakteru Kodeksu, zawiera on wyraźne postanowienie stwierdzające wprost, że jest to kodeks postępowania w rozumieniu art. 40 RODO (ust. 3 Wprowadzenia).

W odniesieniu do podmiotowego zakresu zastosowania Kodeksu zostało przyjęte, iż ma on zastosowanie do banków krajowych oraz rejestrów kredytowych działających na terytorium Rzeczpospolitej Polskiej, będących członkami Związku Banków Polskich (ust. 4 Wprowadzenia). Kodeks zawiera przy tym postanowienie wskazujące, że banki i rejestry kredytowe przetwarzają dane osobowe w związku z prowadzeniem swojej działalności zgodnie z przepisami ustawy z 29.8.1997 r. – Prawo bankowe[37] oraz innych właściwych ustaw oraz w zakresie działalności wynikającej ze swoich statutów z uwzględnieniem wytycznych i rekomendacji Komisji Nadzoru Finansowego oraz innych właściwych regulatorów (ust. 5 Wprowadzenia).

Co istotne, do stosowania Kodeksu mogą przystąpić również inne niż wyżej wskazane podmioty – dotyczy to w szczególności podmiotów świadczących na rzecz banków i rejestrów kredytowych usługi wymagające przetwarzania danych osobowych, jednakże wyłącznie w zakresie świadczenia takich usług na rzecz banków i rejestrów kredytowych (ust. 6 Wprowadzenia). Przystępując do stosowania Kodeksu, tak określone podmioty zobowiązują się do stosowania wszystkich wyrażonych w nim zasad – w celu przystąpienia do stosowania Kodeksu, właściwy podmiot składa bowiem do Związku Banków Polskich pisemne oświadczenie zawierające zobowiązanie do przestrzegania zasad Kodeksu (ust. 9 Wprowadzenia).

W odniesieniu do zakresu przedmiotowego Kodeksu zostało przyjęte, iż będzie mieć on zastosowanie do przetwarzania danych osobowych Klientów[38], w tym osób, których dane są przetwarzane przez rejestry kredytowe w związku z realizacją przez te rejestry obowiązków i uprawnień wskazanych we właściwych przepisach prawa oraz w aktach wewnętrznych (ust. 7 Wprowadzenia). Jednocześnie Kodeks przewiduje wyraźne wyłączenie – nie ma on mianowicie zastosowania do przetwarzania danych osobowych pracowników, współpracowników oraz kandydatów do pracy w bankach i rejestrach kredytowych (ust. 8 Wprowadzenia).

Główne cele, które mają zostać osiągnięte przez wprowadzenie Kodeksu, zostały określone jako (ust. 10 Wprowadzenia):

– wsparcie banków i rejestrów kredytowych we właściwym stosowaniu RODO z uwzględnieniem cech przetwarzania danych osobowych w sektorze bankowym i szczególnych potrzeb banków i rejestrów kredytowych;

[34] Zob. informację o przedmiotowych warsztatach: https://www.giodo.gov.pl/pl/1520310/10311 (dostęp z 27.4.2018 r.).

[35] *P. Litwiński* (red.), Rozporządzenie…, s. 597.

[36] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 819.

[37] T.j. Dz.U. z 2018 r. poz. 2187 ze zm.

[38] Na gruncie Kodeksu zostało przyjęte, że klient oznacza potencjalnego, aktualnego lub byłego: a) klienta banku oraz jego przedstawicieli, osobę korzystającą z usług świadczonych przez banki niebędącą klientem banku lub osobę, której dane osobowe bank przetwarza w związku z prowadzeniem przez bank działalności obejmujących czynności bankowe oraz w związku z realizacją przez bank obowiązków i uprawnień wskazanych we właściwych przepisach prawa, mających zastosowanie do banków oraz w aktach wewnętrznych banków, takich w szczególności jak statuty (klient banku); b) klienta rejestru kredytowego oraz jego przedstawicieli, osobę korzystającą z usług świadczonych przez rejestr kredytowy niebędącą klientem rejestru kredytowego lub osobę, której dane osobowe rejestr kredytowy przetwarza w związku z prowadzeniem przez rejestr kredytowy działalności oraz w związku z realizacją przez rejestr kredytowy obowiązków i uprawnień wskazanych we właściwych przepisach prawa, mających zastosowanie do rejestrów kredytowych (klient rejestru kredytowego).

– dopasowanie obowiązków banków i rejestrów kredytowych oraz podmiotów przetwarzających do wymogów odnoszących się do ryzyka naruszenia praw i wolności osób fizycznych, które może nieść przetwarzanie ich danych osobowych;
– ograniczanie ryzyka naruszenia praw i wolności osób fizycznych, które może nieść przetwarzanie danych osobowych, poprzez wskazanie obowiązków dla banków i rejestrów kredytowych oraz podmiotów przetwarzających dane osobowe w tym zakresie;
– ułatwienie klientom dokonania oceny, czy dany bank lub rejestr kredytowy stosuje odpowiednie zasady ochrony przetwarzanych danych osobowych;
– zwiększenie zaufania klientów do banków oraz rejestrów kredytowych, że ich dane osobowe są chronione na odpowiednim poziomie.

Należy przy tym zauważyć, iż wyżej zarysowane cele wprowadzenia Kodeksu stanowią kolejne bezpośrednie nawiązanie do charakterystyki instytucji kodeksu postępowania określonej na gruncie motywu 98 RODO i art. 40 ust. 1 RODO, w szczególności w obszarze wyjaśniania oraz dostosowania wymogów RODO do konkretnego sektora i związanej z nim specyfiki[39].

Główne elementy „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe"

Oprócz wprowadzenia, które zostało opisane już wcześniej, na Kodeks składa się osiem głównych części tematycznych podzielonych na szczegółowe rozdziały.

Pierwsza część Kodeksu (Część A) stanowi zbiór definicji i skrótów używanych na jego gruncie. Oprócz skrótów dotyczących aktów prawnych, na które powołuje się Kodeks, tak określony słowniczek obejmuje definicje: administratora, danych osobowych, profilowania, pseudonimizacji, zgody, organu nadzorczego, rejestru kredytowego, klienta oraz grupy. Z wyjątkiem trzech ostatnich wszystkie ww. definicje stanowią powtórzenie definicji zawartych w art. 4 RODO. Co istotne, w celu uniknięcia jakichkolwiek wątpliwości zawarte zostało wyraźne zastrzeżenie, iż inne pojęcia użyte w Kodeksie bez nadania im odrębnej definicji mają znaczenie, które zostało im nadane w przepisach RODO.

Kolejna część Kodeksu (Część B) odnosi się do trzech kluczowych zagadnień omawianych w odrębnych, dedykowanych im rozdziałach, tj.: (I) zasad dotyczących przetwarzania danych osobowych; (II) podstaw prawnych przetwarzania danych osobowych; (III) warunków pozyskiwania zgody na przetwarzanie danych osobowych. W ramach pierwszego z ww. rozdziałów Kodeks wymienia oraz opisuje podstawowe zasady dotyczące przetwarzania danych osobowych, tj.: zasadę zgodności z prawem, rzetelności i przejrzystości; zasadę ograniczenia celu przetwarzania; zasadę minimalizacji danych; zasadę prawidłowości; zasadę ograniczenia przechowywania; zasadę integralności i poufności, jak również zasadę rozliczalności. W drugim rozdziale zostają omówione podstawy prawne przetwarzania danych osobowych. W tym też względzie Kodeks wskazuje warunki, przy których spełnieniu bank lub rejestr kredytowy przetwarza dane osobowe. Podstawy prawne przetwarzania danych osobowych zawarte w Kodeksie są przy tym analogiczne do podstaw przetwarzania danych osobowych przewidzianych na gruncie art. 6 ust. 1 RODO. Trzeci rozdział omawia zaś warunki pozyskiwania zgody na przetwarzanie danych osobowych. Jak już zostało wcześniej nadmienione, na gruncie Kodeksu – tak jak w przypadku art. 4 pkt 11 RODO – przez zgodę osoby, której dane dotyczą, należy rozumieć dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. W tym też względzie Kodeks zawiera szczegółowe postanowienia określające m.in.: moment wyrażenia zgody; formę oraz sposoby sformułowania zapytań o zgodę; formę oraz sposoby sformułowania zgody; katalog przykładowych działań klienta, które można uznać za wyraźne działania wskazujące na wyrażenie przez niego zgody; przykłady sytuacji, w których jedna zgoda klienta może obejmować wiele podobnych celów; przykłady sytuacji, których nie należy uznawać za wyrażenie zgody przez klienta; szczegółowe przypadki, w których zgody klienta nie uważa się za wyrażoną świadomie lub dobrowolnie; postanowienia dotyczące przykładowych sposobów wycofania uprzednio wyrażonej zgody; powinności banku lub rejestru kredytowego związane ze zbieraniem zgody lub oświadczenia o wycofaniu zgody.

Następna część Kodeksu (Część C) poświęcona jest niezwykle istotnemu zagadnieniu praw osoby, której dane dotyczą. W tym też względzie Kodeks w szczegółowy, wszechstronny sposób określa zasady oraz sposób realizacji przez banki i rejestry kredytowe praw osób, których dane dotyczą, przy czym każde z omawianych praw zostało opisane w odrębnym, dedykowanym mu rozdziale. Co istotne, Kodeks określa zarówno zasady ogólne – wspólne dla wszystkich omawianych praw, jak i szczegółowe postanowienia dotyczące realizacji poszczególnych praw, uwzględniające ich specyfikę. W powyższym zakresie regulacje Kodeksu obejmują: obowiązek informacyjny; prawo dostępu do danych osoby, której dane dotyczą; prawo do sprostowania danych; prawo do usunięcia danych (prawo do bycia zapomnianym);

[39] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 819.

prawo do ograniczenia przetwarzania danych osobowych; obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania; prawo do przenoszenia danych (w tym: prawo do otrzymywania danych oraz prawo do żądania do przesłania danych innemu administratorowi); prawo sprzeciwu.

Kodeks zawiera również szczegółowe regulacje dotyczące przechowywania i usuwania danych osobowych (Część D), wychodząc z ogólnej zasady, iż dane osobowe klientów lub potencjalnych klientów nie mogą być przechowywane w formie umożliwiającej ich identyfikację przez okres dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. W tym też względzie Kodeks podkreśla m.in., iż po osiągnięciu zamierzonych (pierwotnych) celów przetwarzania, o których mowa wyżej, dane osobowe osób, których dane dotyczą, powinny zostać usunięte, chyba że ich dalsze przechowywanie znajduje podstawę prawną. Jako przykłady tak określonej podstawy prawnej Kodeks podaje ustawę z 29.9.1994 r. o rachunkowości, ustawę z 29.8.1997 r. – Ordynacja podatkowa[40], ustawę z 1.3.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[41] czy też ustawę z 24.11.2017 r. o zmianie niektórych ustaw w celu przeciwdziałania wykorzystywaniu sektora finansowego do wyłudzeń skarbowych[42].

Jednym z najistotniejszych obszarów tematycznych regulowanych przez Kodeks jest instytucja profilowania oraz zautomatyzowanego przetwarzania danych osobowych osób fizycznych (Część E). W tym też względzie Kodeks zawiera zbiór zasad dotyczących procesu profilowania oraz zautomatyzowanego przetwarzania danych osobowych, wskazując, że profilowanie jest metodą przetwarzania danych osobowych, które może być oparte na różnych modelach oraz algorytmach. W szczególności Kodeks podkreśla, że profilowanie opiera się na odpowiednich matematycznych lub statystycznych procedurach profilowania, z zachowaniem środków technicznych i organizacyjnych zapewniających zmniejszenie ryzyka błędów w procedurach profilowania. Kodeks wyraża ponadto zasadę, iż do profilowania banki i rejestry kredytowe wykorzystują dane osobowe osoby, której dane dotyczą, i dane o jej zobowiązaniach (w tym historię kredytową klienta) w takim zakresie, w jakim przetwarzanie tych danych jest niezbędne i adekwatne do celu przetwarzania. Należy przy tym wskazać, że Kodeks zawiera niezwykle szeroki katalog przykładowych celów profilowania klientów przez banki oraz rejestry kredytowe – stanowi to również odzwierciedlenie informacyjnej funkcji Kodeksu, w ramach której klient będzie mógł poprzez treść Kodeksu zapoznać się z przykładami sytuacji, w których banki oraz rejestry kredytowe dokonują profilowania. W podobnym kontekście należy również odczytywać przewidziany w Kodeksie katalog przykładowych działań dotyczących procesu oceny zdolności i wiarygodności kredytowej klienta, w związku z którymi wykorzystywana jest ocena punktowa klienta lub inny profil udostępniony przez rejestr kredytowy czy też będący wynikiem profilowania przez bank zgodnie z modelami własnymi banku. W bezpośrednim nawiązaniu do wyżej zarysowanych zagadnień Kodeks zawiera również – w formie załączników – opis modelu oceny punktowej (scoringowego) wykorzystywanego w procesie zarządzania ryzykiem kredytowym (Załącznik Nr 3) oraz przykłady zautomatyzowanego przetwarzania danych (Załącznik Nr 6).

Kodeks odnosi się również do zagadnienia powierzenia przetwarzania danych osobowych w kontekście klauzul umów z dostawcami (Część F). Na gruncie Kodeksu przewidziane jest bowiem, iż banki jako administratorzy mogą stosować do umów zawieranych z podmiotami przetwarzającymi przykładowe zapisy wymienione w Załączniku Nr 5 do Kodeksu – z zastrzeżeniem, że w przypadku wydania przez Komisję Europejską lub organ nadzoru standardowych klauzul umownych mają one pierwszeństwo przed postanowieniami Kodeksu. Kodeks podkreśla przy tym, iż przewidziane w nim standardowe klauzule umowne mają charakter przykładowy i nie wyłączają prawa banku do zastosowania we własnych umowach z podmiotami przetwarzającymi dane odmiennych klauzul.

Kodeks określa również zasady dotyczące powiadomienia o naruszeniu ochrony danych osobowych (Część G). W tym względzie Kodeks zawiera postanowienia dotyczące zarówno sytuacji naruszenia ochrony danych osobowych podlegającego obowiązkowi zgłoszenia organowi nadzorczemu, jak i naruszenia ochrony danych osobowych podlegającego obowiązkowi zgłoszenia osobie, której dane dotyczą. Na gruncie Kodeksu przyjęto, że naruszenie ochrony danych osobowych w bankach i rejestrach kredytowych rozpatrywane jest jako zdarzenie występujące w ramach ryzyka operacyjnego, które należy rozumieć jako możliwość wystąpienia straty wynikającej z niedostosowania lub zawodności procesów wewnętrznych, ludzi i systemów lub ze zdarzeń zewnętrznych. Kodeks doprecyzowuje przy tym, iż naruszeniem ochrony danych osobowych jest 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 w ramach prowadzonej przez administratora danych działalności. Co istotne, Kodeks zawiera m.in. przykłady sytuacji, które mogą prowadzić do naruszenia ochrony danych osobowych, jak również przykłady przypadków stanowiących naruszenie ochrony danych osobowych podlegające obowiązkowi zgłoszenia organowi nadzorczemu oraz przykłady przypadków stanowiących naruszenie ochrony danych osobowych podlegające obowiązkowi zgłoszenia osobie, której dane dotyczą. W powyższym kontekście warto również podkreślić, iż jednymi z załączników do Ko-

[40] T.j. Dz.U. z 2018 r. poz. 800 ze zm.
[41] Dz.U. poz. 723.
[42] Dz.U. poz. 2491 ze zm.

deksu są: wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie organu nadzorczego (Załącznik Nr 1), jak również wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie osoby, której dane dotyczą (Załącznik Nr 2).

Ostatnim obszarem regulowanym przez Kodeks jest zaś zagadnienie oceny skutków przetwarzania danych (Część H), w ramach którego Kodeks m.in. wskazuje przykłady sytuacji, kiedy banki i rejestry kredytowe powinny rozważyć przeprowadzenie oceny skutków dla ochrony danych osobowych.

Integralną częścią Kodeksu jest również sześć załączników, z których część została już opisana wcześniej. W tym też względzie należy wskazać, że Kodeks zawiera następujące Załączniki:

– Wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie organu nadzorczego (Załącznik Nr 1);
– Wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie osoby, której dane dotyczą (Załącznik Nr 2);
– Opis przykładowego modelu oceny punktowej (scoringowego) wykorzystywanego w procesie zarządzania ryzykiem kredytowym (Załącznik Nr 3);
– Zakresy informacji przekazywanych Klientowi (Załącznik Nr 4);
– Przykładowe postanowienia umów zawieranych z podmiotami przetwarzającymi (Załącznik Nr 5);
– Przykłady zautomatyzowanego przetwarzania danych (Załącznik Nr 6).

Podsumowanie

Kodeksy postępowania stanowią jedną z najważniejszych instytucji przewidzianych na gruncie przepisów RODO. Charakteryzowane jako instrument samoregulacyjny wspomagający oraz usprawniający proces wdrożenia przepisów RODO poprzez dostosowanie wymogów wskazanego rozporządzenia do specyfiki konkretnych sektorów gospodarki[43], kodeksy postępowania mogą stanowić istotne udogodnienie dla wielu kategorii administratorów oraz podmiotów przetwarzających. W tym też kontekście członkowie Związku Banków Polskich – świadomi wyzwań związanych ze skutecznym oraz prawidłowym wdrożeniem RODO – wraz z wejściem RODO rozpoczęli intensywne prace nad projektem kodeksu postępowania dla polskiego sektora bankowego. Efektem tychże prac przeprowadzanych na forum Związku Banków Polskich jest obecny projekt „Kodeksu dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe", który – po przejściu procedury opiniowania oraz zatwierdzania określonej w art. 40 RODO – ma szansę stać się kluczowym instrumentem skutecznie oraz spójnie dostosowującym polski sektor bankowy do wymogów stawianych przez RODO.

[43] *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne…, s. 819.

Słowa kluczowe: RODO, kodeks postępowania, banki, ochrona danych osobowych.

Implementing GDPR in banks based on "The code of good practices in the scope of processing of personal data by banks and credit register"

The aim of the present study is to present the project "The code of good practices in the scope of processing of personal data by banks and credit register" (further referred to as: Code), developed by the Polish Bank Association, as an example of activities implementing regulation of the European Parliament and of the Council 2016/679 of 27.4.2016, in the matter of protection of natural persons in regard to processing of personal data and in the matter of free movement of such data and repealing the directive 95/46/EC (general data protection regulation) in Polish bank sector and its entities. In order to provide direct reference of the abovementioned issue to legislative context in the form of GDPR, discussing contents of the project Code will be preceded by a general characteristics of the institution of the code of conduct based on provisions of the regulation.

Keywords: GDPR, code of conduct, banks, personal data protection.

Dochodzenie roszczeń w aspekcie zapewnienia ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych

dr hab. *Izabella Gil*[1]

W opracowaniu przedstawiono, jakie są zasady prowadzenia korespondencji elektronicznej w ramach wykonywanych przez profesjonalnych pełnomocników czynności. Celem artykułu jest ustalenie, czy adwokat lub radca prawny występuje w roli administratora danych osobowych w przypadku spraw powierzanych do prowadzenia, czy w roli przetwarzającego dane osobowe (procesora). W opracowaniu zwrócono uwagę na możliwości występowania kolizji pomiędzy obowiązkiem ochrony danych osobowych a obowiązkiem zachowania tajemnicy zawodowej przez profesjonalnych pełnomocników.

Uwagi wstępne

Specyfika zawodu radcy prawnego, jak również adwokatów wymaga nie tylko profesjonalnego prowadzenia spraw związanych z dochodzeniem roszczeń jako pełnomocników, ale także przestrzegania przepisów prawa unijnego, krajowego oraz zasad etyki wykonywanego zawodu. Zawodowi pełnomocnicy powinni zapewnić wysoki poziom świadczonej przez daną grupę zawodową pomocy prawnej, mającej na celu ochronę prawną interesów podmiotów, na których rzecz jest wykonywana. Przy czym profesjonalizm przejawia się także w zapewnieniu właściwej ochrony prawnej pozostałym podmiotom uczestniczącym w postępowaniu cywilnym. Wszelkie zawody zaufania publicznego sprawują bowiem pieczę nad należytym wykonywaniem tych zawodów w granicach interesu publicznego i w celu jego ochrony[2]. Ochrona prawna powinna być zapewniona we wszystkich formach wykonywania czynności zawodowych, a więc także przy korzystaniu z narzędzi elektronicznych. Zawodowy pełnomocnik powinien zapewnić w ramach tajemnicy zawodowej również stosowną ochronę danych osobowych przy korzystaniu z poczty elektronicznej i stron internetowych.

Zasady prowadzenia korespondencji elektronicznej w ramach wykonywanych przez profesjonalnych pełnomocników czynności

W momencie zlecenia sprawy do prowadzenia pojawia się konieczność poznania okoliczności faktycznych celem ustalenia formy, sposobu i zakresu ochrony prawnej, jaka ma zostać udzielona mocodawcy, który powierza prowadzenie sprawy cywilnej. Dokonując powyższych ustaleń, zawodowy pełnomocnik uzyskuje również szczegółowe informacje i dane osobowe odnoszące się do przeciwnika procesowego lub uczestnika postępowania, a więc już na tym wstępnym etapie pozyskuje dane osobowe, które mogą podlegać ochronie prawnej. Wprawdzie nie następuje jeszcze etap związany z przetwarzaniem informacji i danych, ale już wówczas pojawia się konieczność zabezpieczenia tych uzyskanych informacji oraz danych. Kolejnym etapem związanym z udzielaną pomocą prawną jest dokonywanie czynności przedprocesowych, np. skierowanie wezwania do dobrowolnej zapłaty lub wezwania do wykupienia weksla. Często już wtedy powstają projekty pism, które są przesyłane w formie elektronicznej do mocodawcy w celu akceptacji lub wyjaśnienia dalszych okoliczności faktycznych, co skutkuje obowiązkiem zabezpieczenia tego rodzaju danych. Stosownie bowiem do art. 35 uchwały Nr 3/2014 Nadzwyczajnego Krajowego Zjazdu Radców Prawnych w sprawie kodeksu etyki radcy prawnego z 22.11.2014 r.[3] – „Radca prawny może wykonywać czynności zawodowe drogą elektroniczną, jeśli:

1) jest zawsze jednoznacznie identyfikowalny jako nadawca lub odbiorca, w szczególności poprzez adresy poczty elektronicznej lub inne identyfikatory;
2) nie korzysta z drogi elektronicznej w sposób anonimowy lub na rzecz osób, których nie można jednoznacznie zidentyfikować jako konkretnych klientów lub odbiorców czy nadawców w komunikacji, w szczególności w Internecie;
3) nie korzysta z form aktywności dostępnych drogą elektroniczną w sposób sprzeczny z prawem, dobrymi obyczajami i zasadami Kodeksu, w szczególności tworząc rozwiązania skutkujące nieprawdziwymi, wprowadzającymi w błąd, ocennymi oznaczeniami lub informacjami, lub

[1] Autorka jest profesorem Uniwersytetu Wrocławskiego, Zakład Postępowania Cywilnego, WPAE.

[2] Por. uzasadnienie wyroku TK z 8.12.1998 r., K 41/97, OTK 1998, Nr 7, poz. 117.

[3] K.Rad.Prawn z 2014 r. poz. 110.

w sposób utrudniający innym radcom prawnym dostęp do rynku;
4) korzysta z form aktywności dostępnych drogą elektroniczną w sposób gwarantujący oddzielenie wykonywania zawodu od swoich prywatnych przekonań, poglądów, postaw i działań oraz innej działalności zawodowej;
5) nie wydaje, nie inspiruje lub nie płaci osobom trzecim za wydawanie pozytywnych lub negatywnych opinii, komentarzy, poleceń, rekomendacji bądź referencji dotyczących wykonywania zawodu przez siebie lub inne osoby, z którymi może na podstawie przepisów prawa wspólnie wykonywać zawód, w szczególności w sposób anonimowy, nieprawdziwy lub wprowadzający w błąd;
6) poprzez okresową archiwizację zabezpiecza i dba o dostępność danych przetwarzanych drogą elektroniczną;
7) chroni tajemnicę zawodową, informując w treści korespondencji elektronicznej o jej poufnym charakterze; zabezpieczenie uznaje się za należyte, jeżeli klient po uprzednim poinformowaniu go o zagrożeniach związanych z korzystaniem z drogi elektronicznej, domyślnie lub wyraźnie zaakceptował stosowane w komunikacji z nim środki, techniki, sposoby, systemy lub standardy komunikacji elektronicznej".

W aspekcie tematu opracowania należy zwrócić uwagę na obowiązek wynikający z pkt 6 i 7 art. 35 Kodeksu Etyki Radcy Prawnego. Wymóg związany z archiwizacją danych ma umożliwić ich weryfikację, czy dane te są poprawne, gdyż zgodnie z art. 5 ust. 1 lit. a) rozporządzenia Parlamentu Europejskiego UE 2016/679 z 27.4.2016 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)[4] – dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"). Osobie, której dane dotyczą, przysługuje tzw. prawo dostępu do danych osobowych (art. 15 RODO[5]).

Dokonywanie archiwizacji danych nie służy jednak tylko ponownemu ich wykorzystaniu w związku ze świadczeniem pomocy prawnej, ale pozwala również ocenić odpowiednie wykonywanie czynności zawodowych przez radcę prawnego.

Jak zasadnie dostrzega się w doktrynie, w przypadku prowadzenia korespondencji elektronicznej w ramach wykonywanych czynności zawodowych konieczne jest:
1) poinformowanie mocodawcy o zagrożeniach związanych z korzystaniem z drogi elektronicznej, w tym związanych z możliwością dostępu osób nieuprawnionych do informacji przekazywanych tą formą z wykorzystaniem nielegalnych środków technicznych, a w tym zakresie poinformowanie klienta, że udziela zgody dorozumianej, jeżeli będzie kontynuował korespondencję;
2) uzyskanie zgody klienta na prowadzenie korespondencji elektronicznej, która może być wyraźna poprzez zamieszczenie tej formy komunikowania się na odległość w treści postanowień umowy, albo w odrębnym dokumencie, albo w sposób dorozumiany w przypadku kontynuowania korespondencji po przekazaniu klientowi informacji o zagrożeniach towarzyszących korzystaniu z poczty elektronicznej[6].

W RODO przewidziane są sankcje za naruszenie uprawnień informacyjnych podmiotu danych i powiązanych z nimi obowiązków informacyjnych administratora danych. Stosownie do art. 83 ust. 5 RODO naruszenie przepisów dotyczących m.in. obowiązków informacyjnych może skutkować wymierzeniem przez organ nadzorczy administracyjnej kary pieniężnej w wysokości do 20 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Celem takiej regulacji (por. motyw 148 RODO) jest wzmocnienie skuteczności stosowania RODO. Ustawodawca unijny wprowadził uprawnienie do nakładania administracyjnych kar pieniężnych dla każdego organu nadzorczego w każdym państwie członkowskim[7]. Dążac do harmonizacji i wzmocnienia sankcji przewidzianych w rozporządzeniu (motyw 150 preambuły RODO) sankcje administracyjne i odpowiedzialność karną uregulowano w przepisach ustawy z 10.5.2018 r. o ochronie danych osobowych (rozdział 11)[8]. W literaturze podkreśla się, że

[4] Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

[5] Zgodnie z art. 15 RODO „1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji: a) cele przetwarzania; b) kategorie odnośnych danych osobowych; c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych; d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu; e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania; f) informacje o prawie wniesienia skargi do organu nadzorczego; g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle; h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą".

[6] *G. Dźwigała*, [w:] *T. Scheffler* (red.), Komentarz do art. 35 KERP, Kodeks Etyki Radcy Prawnego. Komentarz, Warszawa 2017, wyd. 2/uwaga Nr 23.

[7] *B. Marcinkowski*, ustawa o ochronie danych osobowych. Komentarz, LEX, https://sip.lex.pl/#/commentary/587775699/573139/marcinkowski-bartosz-red-ustawa-o-ochronie-danych-osobowych-komentarz?cm=URELATIONS (dostęp z 11.1.2019 r.).

[8] Dz.U. poz. 1000 ze zm.

w zamierzeniu unijnego prawodawcy wprowadzenie tak wysokich kar pieniężnych ma mieć m.in. charakter odstraszający i skłonić administratorów danych do wypełniania obowiązków nałożonych przepisami RODO[9].

Specyfika zawodu radcy prawnego, jak też adwokatów a ochrona danych osobowych

Administratorem danych osobowych w przypadku zawodowych pełnomocników i powierzanych im do prowadzenia spraw będą osoby zlecające (powierzające) sprawę do prowadzenia (klienci). Pełnomocnik wprawdzie uzyskuje także informacje i dane osobowe odnoszące się do przeciwnika procesowego lub uczestnika postępowania, ale przetwarza je na potrzeby prowadzonej sprawy i zgodnie z wolą mocodawcy (pełnomocnik działa bowiem w cudzym imieniu i na cudzy rachunek). Zgodnie z art. 4 pkt 7 RODO – za administratora danych osobowych uważa się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administrator określa zatem, co stanie się z danymi osobowymi, w jaki sposób to nastąpi, kto będzie uprawniony do ich przetwarzania, jak należy dane osobowe zabezpieczyć, natomiast podmiot przetwarzający działa na podstawie umowy z administratorem danych, który powierzył mu przetwarzanie danych w określonym zakresie. Wprawdzie adwokatowi lub radcy prawnemu jako pełnomocnikowi, w związku ze świadczeniem pomocy prawnej na rzecz osoby udzielającej pełnomocnictwa, przekazywane są dane innych osób, ale będą one przetwarzane celem należytego poprowadzenia powierzonej mu sprawy. Podejmując czynności związane z prowadzeniem sprawy zawodowy pełnomocnik powinien więc powołać się na podstawę przetwarzania danych osobowych związaną z koniecznością podania danych osobowych przy poszczególnych czynnościach procesowych. Z powyższych względów w umowie zawieranej z klientem należałoby zawrzeć postanowienia odnoszące się do przetwarzania danych osobowych w celu związanym z prowadzeniem sprawy (w tym dochodzeniem roszczeń, udzielania porad prawnych, sporządzania opinii prawnych).

Niewątpliwie ww. relacje utrudniają jednoznaczne ustalenie, czy adwokat lub radca prawny występuje w roli administratora danych osobowych w przypadku spraw powierzanych do prowadzenia, czy w roli przetwarzającego dane osobowe (procesora). Ponadto na złożoność owych relacji nakłada się jeszcze problem związany z przestrzeganiem tajemnicy zawodowej. Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO[10] uwzględnia specyfikę czynności zawodowych pełnomocników (adwokatów i radców prawnych). Zarówno bowiem w ustawie z 26.5.1982 r. – Prawo o adwokaturze[11], jak i ustawie z 6.7.1982 r. – o Radcach prawnych[12] projekt przewiduje dodanie działu regulującego zagadnienie przetwarzania danych osobowych. I tak, według projektowanego art. 16a ustawy Prawo o adwokaturze (odpowiednio art. 5a ustawy o Radcach prawnych), art. 15 ust. 1 i 3, art. 18 i art. 19 RODO będą miały zastosowanie w zakresie, w jakim nie naruszają obowiązku zachowania przez adwokata tajemnicy zawodowej, a ponadto nie będzie miał zastosowania art. 21 ust. 1 RODO w przypadku danych osobowych pozyskanych przez adwokata w związku z udzielaniem pomocy prawnej. W uzasadnieniu ww. projektu UC 100 (druk Nr 3050) podkreślono, że projektowane zmiany (zawarte w art. 7 i 8) związane z wprowadzeniem ograniczeń w zakresie ochrony danych osobowych ze względu na konieczność przestrzegania tajemnicy zawodowej przez profesjonalnych pełnomocników, mieszczą się w katalogu określonym w art. 23 ust. 1 RODO, nie wykraczają poza zakres określony w Konstytucji RP, a także są zgodne z zasadą proporcjonalności[13]. Projektowane regulacje mogą ograniczać prawa osób, których dane osobowe dotyczą (np. osoby trzeciej, a nie klienta), jednakże są konieczne ze względu na zapewnienie prawidłowego wykonywania przez adwokatów i radców prawnych obowiązku zachowania tajemnicy zawodowej.

Przetwarzanie danych osobowych

Przepisy RODO znajdują zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych (art. 2 ust. 1 RODO). Oznacza to, że przetwarzanie uzyskanych danych osobowych może nastąpić w sposób całkowicie lub częściowo zautomatyzowany (przy użyciu elektronicznej, edytorów tekstów, programów, np. Kancelaris itp.), a także w inny sposób (np. wykonania kopii czy skanów dokumentów, ich broszurowania poprzez zakładanie akt). Dane w postaci papierowej podlegają ochronie nie tylko wtedy, gdy stanowią część zbioru danych, ale także wtedy, gdy mają sta-

[9] *P. Figielski*, Obowiązek informacyjny w ogólnym rozporządzeniu o ochronie danych, Informacja w Administracji Państwowej (IAP) 2017, Nr 1, s. 23.

[10] Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 Nr UC 100 Ministra Cyfryzacji – zob. https://legislacja.rcl.gov.pl/projekt/12302951 (dostęp z 10.1.2019 r.).

[11] T.j. Dz.U. z 2018 r. poz. 1184 ze zm.

[12] T.j. Dz.U. z 2018 r. poz. 2115 ze zm.

[13] Uzasadnienie projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 Nr UC 100 Ministra Cyfryzacji – zob. http://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=3050 (dostęp z 11.1.2019 r.).

nowić część zbioru, czyli uporządkowanego zestawu danych osobowych dostępnych według określonych kryteriów (art. 4 pkt 6 RODO). W związku z powyższym za zbiór danych osobowych należy uznać „każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy też podzielony funkcjonalnie. Zbiór akt postępowania administracyjnego, zawierając dane stron, ich adresy i inne informacje, spełnia te kryteria i wobec tego jest zbiorem danych w rozumieniu ustawy”[14]. Wszelkie materiały, które są gromadzone w formie akt, w tym sądowe prokuratorskie, policyjne i inne zawierające dane osobowe, są zbiorem danych osobowych[15].

Otrzymując informacje w momencie przyjęcia sprawy do prowadzenia, dochodzi do przetwarzania danych osobowych, w tym poprzez przygotowywanie pism procesowych. Zgodnie z art. 4 pkt 2 RODO „przetwarzanie” oznacza bowiem operację lub zestaw operacji wykonywanych na danych osobowych bądź 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. Podmiotem, który przetwarza dane osobowe, czyli „podmiotem przetwarzającym” jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt 8 RODO).

Zgodnie z art. 28 ust. 3 RODO przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

a) „przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora (…);
b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmuje wszelkie środki wymagane na mocy art. 32;
d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;
e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;
f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;
g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich”.

Stosownie do art. 28 ust. 2 RODO podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. Z powyższych względów w umowie z klientem należałoby zaznaczyć, że wyraża on zgodę na przetwarzanie przekazanych danych przez pracowników kancelarii lub osoby współpracujące. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. W związku z taką regulacją pełnomocnik powinien powiadomić klienta o zamiarze skorzystania z zastępstwa procesowego przez innego radcę prawnego czy adwokata, jak też aplikantów. Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają na mocy umowy te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym. W szczególności nałożony zostaje obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarza-

[14] Sprawozdanie Generalnego Inspektora Ochrony Danych Osobowych za rok 1999, s. 17.

[15] Por. stanowisko Generalnego Inspektora Ochrony Danych Osobowych dostępne na stronie www.giodo.gov.pl, dostęp 8.11.2017 r., w dziale Odpowiedzi na pytania.

jącego spoczywa na pierwotnym podmiocie przetwarzającym (art. 28 ust. 4 RODO).

Kolejnym etapem związanym z przetwarzaniem danych osobowych w przypadku świadczenia pomocy prawnej jest ich zamieszczenie w pismach inicjujących postępowanie cywilne (pozwach lub wnioskach składanych w postępowaniu nieprocesowym czy postępowaniach pomocniczych), czy też składanych w związku z zaskarżaniem rozstrzygnięć w imieniu klienta.

W myśl art. 4 pkt 1 RODO przez dane osobowe należy rozumieć informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, a więc *a contrario* nie stanowią danych osobowych w rozumieniu RODO informacje odnoszące się do osób prawnych. Z tym zastrzeżeniem, że ujawnianie informacji dotyczących osób fizycznych wchodzących w skład organów można uznać za dane osobowe. Mając na uwadze powyższą regulację, ochronie danych osobowych będą zatem podlegały także informacje o osobach prowadzących indywidualną działalność gospodarczą. Regulacje RODO powodują, że każdorazowo pojawi się konieczność ustalenia, czy podanie imienia i nazwiska umożliwia zidentyfikowanie osoby. W doktrynie zasadnie dostrzeżono, że ponadto wszystko będzie zależało od odbiorcy, do którego danego rodzaju informacja trafia, jak np. w odniesieniu do danych specjalistycznych czy danych dotyczących podawania REGONU lub NIP w numerze faktury, gdyż dane tego rodzaju określa się mianem relatywizacji danych osobowych[16].

Dochodzenie roszczeń wiąże się z koniecznością przedstawienia danych zarówno po stronie powodowej, jak i po stronie pozwanej. Pozwalają one bowiem na zidentyfikowanie podmiotu wszczynającego postępowanie, jak też podmiotu przeciwko któremu prowadzone jest postępowanie cywilne. Dochodzenie roszczeń uznawane jest za dopuszczalne i zgodne z prawem przetwarzanie danych osobowych[17]. Dochodzenie roszczeń zostało wprost wskazane jako okoliczność uzasadniająca przetwarzanie danych [art. 9 ust. 2 lit. f) RODO], a więc znajduje swoją normatywną podstawę. Ponadto przetwarzanie danych osobowych jest zgodne z prawem także wtedy, gdy na takie przetwarzanie zezwalają szczególne przepisy prawa [por. art. 6 ust. 1 lit. c) i art. 9 ust. 2 lit. g) RODO]. Przepisy Kodeksu postępowania cywilnego określają konkretny zakres danych osobowych, jaki powinien zostać podany w związku z konkretnymi czynnościami procesowymi. Przykładowo na mocy art. 126 § 1 i 2 KPC należy podać PESEL lub NIP, które zostaną zamieszczone w postanowieniu o nadaniu klauzuli wykonalności, a uwidaczniane są na pismach procesowych. Trzeba także mieć na uwadze, że RODO wyodrębnia dane zwykłe oraz tzw. dane wrażliwe.

Obowiązki związane z przetwarzaniem danych osobowych

Regulacja zawarta w RODO określa obowiązki związane z przetwarzaniem danych osobowych, a wśród nich wspomniany obowiązek zgodności z prawem przetwarzania danych osobowych, obowiązek informacyjny i inne obowiązki wobec osób, których dane dotyczą, obowiązek przeprowadzenia oceny skutków dla ochrony danych osobowych, obowiązek zabezpieczenia danych osobowych.

Przetwarzanie jest w świetle regulacji RODO traktowane jako zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Skoro przetwarzanie danych osobowych zwykłych jest dopuszczalne m.in. wtedy, gdy jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora, to pełnomocnik może przetwarzać dane osobowe przekazane mu przez klienta.

Na mocy art. 17 ust. 1 RODO osoba trzecia (strona lub uczestnik postępowania), której dane dotyczą, mogłaby żądać od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator miałby obowiązek bez

[16] Więcej na ten temat por. zob. *W. Zimny*, Praktyczne skutki nowelizacji ustawy o ochronie danych osobowych z 25.8.2001 r., Ochrona Danych Osobowych. Biuletyn ABI 2001, Nr 21, s. 3.

[17] Zob. *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive* 95/46/EC, WP 217, s. 61.

zbędnej zwłoki usunąć dane osobowe, jeżeli zachodziłaby jedna z okoliczności wymienionych w tym przepisie. W związku z taką regulacją klientowi (jako administratorowi) powinny zostać przekazane akta sprawy na jego żądanie. Po zakończeniu prowadzenia sprawy zawodowi pełnomocnicy również powinni przekazać swojemu mocodawcy (administratorowi danych) dokumenty, w których zawarte są dane osobowe, gdyż odpadł cel stanowiący podstawę do ich przetwarzania. Po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora należy usunąć lub zwrócić administratorowi wszelkie dane osobowe oraz usunąć wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

Ocena skutków przetwarzania

Na zakończenie należy jeszcze rozważyć, czy zgodnie z art. 35 ust. 1 i 3 RODO wymagane będzie przeprowadzenie oceny skutków dla ochrony danych. Oceny skutków dokonuje się obowiązkowo m.in. w przypadku przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO. A zatem istotne będzie ustalenie, czy przetwarzanie danych osobowych następuje na dużą skalę. W związku z tym w przypadku kancelarii, które nie zajmują się przetwarzaniem danych na „dużą skalę", nie pojawi się konieczność przeprowadzenia oceny skutków dla ochrony danych.

Z uwagi na fakt, że to administrator danych osobowych ponosi odpowiedzialność za wybór właściwego podmiotu przetwarzającego dane na jego zlecenie, to o powierzeniu prowadzenia sprawy do prowadzenia będzie decydował także sposób gwarancji związanych z zabezpieczeniem danych osobowych. Zgodnie z art. 28 ust. 1 RODO, jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. Administrator danych, dokonując wyboru podmiotów przetwarzających dane osobowe, powinien uwzględniać w szczególności poziom zabezpieczenia danych osobowych oferowany przez procesora.

Należy także mieć na uwadze, że stosownie do art. 58 ust. 1 RODO każdemu organowi nadzorczemu przysługują następujące uprawnienia w zakresie prowadzonych postępowań:

a) nakazanie administratorowi i podmiotowi przetwarzającemu, a w stosownym przypadku przedstawicielowi administratora lub podmiotu przetwarzającego, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań;
b) prowadzenie postępowań w formie audytów ochrony danych;
c) dokonywanie przeglądu udzielonych certyfikacji na mocy art. 42 ust. 7;
d) zawiadamianie administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia niniejszego rozporządzenia.

W przypadku danych osobowych, które radca prawny, adwokat jako podmiot przetwarzający otrzymali lub pozyskali w wyniku lub w ramach działania objętego obowiązkiem zachowania tajemnicy zawodowej, art. 58 ust. 1 lit. e) i f) RODO się nie stosuje. Oznacza to, że organ nadzorczy nie może uzyskiwać od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań ani uzyskiwać dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego.

Podsumowanie

Wskutek przyjęcia przez zawodowego pełnomocnika sprawy do prowadzenia jest on związany tajemnicą zawodową i dlatego stosowanie wszystkich przepisów RODO mogłoby doprowadzić do jej naruszenia. W wielu przypadkach, w celu zapewnienia należytej ochrony prawnej, pełnomocnicy muszą przetwarzać dane osobowe innych podmiotów niż osoba udzielająca pełnomocnictwa. Wówczas dochodzić może do konieczności wyważenia interesów klienta w relacji do prawa ochrony danych osobowych, osób, których dane zostały pełnomocnikowi przekazane. Czynności związane z udzielaniem pomocy prawnej, w tym także uzyskiwanie danych osobowych, należy oceniać w różnych relacjach występujących nie tylko z klientem, ale także z organami postępowania, z pracownikami pełnomocnika czy innymi pełnomocnikami (mogącymi zastępować w czynnościach w ramach pełnomocnictwa substytucyjnego), jak też w relacjach z innymi stronami lub uczestnikami postępowania. Tego rodzaju różne relacje powodują, że zakres ochrony danych osobowych też będzie kształtował się odmiennie. W relacji z klientem (w związku z prowadzeniem sprawy) adwokat czy radca prawny będzie występował w roli procesora (przetwarzającego uzyskane dane osobowe). Natomiast w relacji z pracownikami kancelarii czy też osób współpracujących będzie działał jak administrator danych, gdyż będzie określał, co stanie się z danymi osobowymi klienta, w jaki sposób to nastąpi, kto będzie uprawniony do ich przetwarzania, jak należy dane osobowe zabezpieczyć.

Słowa kluczowe: adwokat, radca prawny, dane osobowe, administrator, procesor.

Redress in the aspect of providing protection of natural persons in regard to processing of personal data

The study presents the principles of conducting electronic correspondence as a part of activities carried out by professional attorneys. The purpose of the article is to determine whether a lawyer or legal counsel acts as a personal data administrator in regard to cases they are entrusted to conduct, or in the role of a person processing personal data (processor). The study points out the possibility of collisions between the obligation to protect personal data and the obligation of professional secrecy by professional attorneys.

Keywords: lawyer, legal counsel, personal data, administrator, processor.

Informatyzacja zasobów podmiotów wykonujących działalność leczniczą. Interoperacyjność i ochrona danych – jak to działa?

Kajetan Wojsyk[1]

Celem niniejszego opracowania jest zwrócenie uwagi na specyfikę bardzo złożonego systemu, jakim jest system informacji w ochronie zdrowia, w ramach którego dochodzi do przetwarzania danych. Po pierwsze, chodzi tutaj o dane, których powszechne i bezwarunkowe udostępnienie stanowi korzyść społeczną i które mogą być wykorzystywane do różnych celów, niekoniecznie jedynie tego, dla którego system ten został stworzony. Po drugie, są to dane, które muszą być chronione, gdyż są danymi osobowymi, w tym danymi szczególnych kategorii.

Uwagi wstępne

System informacji w ochronie zdrowia regulowany jest ustawą z 28.4.2011 r. o systemie informacji w ochronie zdrowia[2]. Jego funkcjonalność jest uzależniona od jakości i kompletności elementów składowych – różnego rodzaju rejestrów podmiotowych i przedmiotowych, w tym także rejestrów funkcjonujących w ramach odrębnych systemów. Rejestry te należy traktować jako swoiste zbiory danych gromadzonych dla osiągnięcia konkretnych celów, również regulowanych ustawowo. Trzeba równocześnie umieć świadomość, że owe rejestry tworzone były w różnym czasie, w oparciu na różne podstawy prawne oraz technologie – i co do zasady są autonomiczne. Jednak systematyczna informatyzacja obszarów bezpośrednio niezwiązanych z ochroną zdrowia (np. ewidencji działalności gospodarczej, ewidencji ludności, ewidencji podatników, statystyki) pozwala na kreowanie większych przestrzeni informacyjnych, w których można tworzyć systemy o znacznie większej przydatności i użyteczności funkcjonalnej. W tym kontekście niezwykle istotne było wprowadzenie podstawy prawnej tzw. interoperacyjności systemów[3]. Interoperacyjność to zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych[4].

Separacja danych, szyfrowanie, bezpieczne przechowywanie danych oraz dokumentów

Systemu informacji w ochronie zdrowia nie należy pojmować jako jednolitego systemu o ściśle określonej strukturze, systemu, którego poszczególne elementy składowe daje się jednoznacznie i raz na zawsze opisać. Jest on raczej stale zmieniającym się systemem rozproszonym, którego granice systematycznie się poszerzają, a elementy składowe muszą podlegać stałej poprawie jakości. Aby dokładniej wyobrazić sobie specyfikę tego systemu, wystarczy przyjąć, że jego istotą jest gromadzenie i przetwarzanie danych dotyczących stanu zdrowia i historii leczenia osób fizycznych, z uwzględnieniem nie tylko tych danych, ale także danych opisujących miejsca wykonywania działalności leczniczej, osób wykonujących tę działalność (pracowników medycznych i pracowników pomocniczych), przepływu środków finansowych związanych z realizacją poszczególnych procedur leczniczych, rejestracji okresów niezdolności do pracy i wielu jeszcze innych danych.

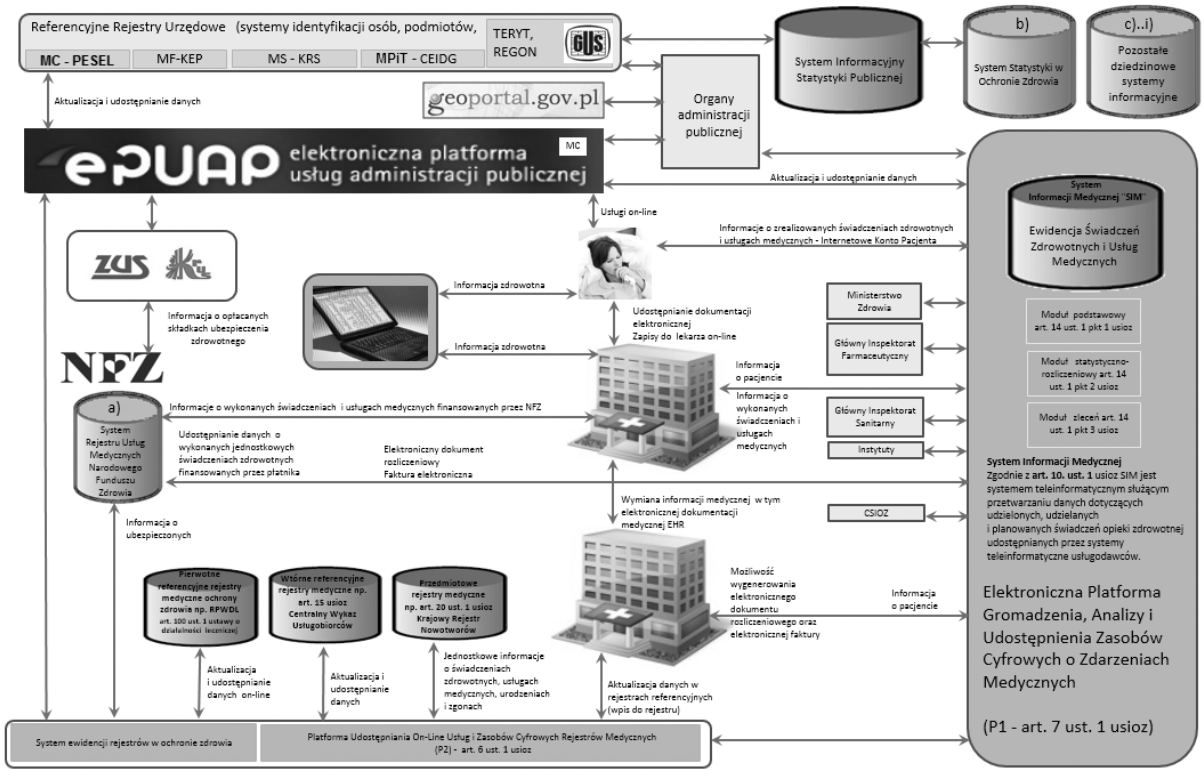
Jest kwestią oczywistą, że owa różnorodność danych wymaga odpowiedniej organizacji sposobu ich gromadzenia, porządkowania, bezpiecznego przechowywania i udostępniania osobom uprawnionym. Wymagane jest też pewne i wyraźne kanalizowanie przepływu danych i informacji, by zachować funkcjonalność, jaką jest separacja danych chronionych, a z drugiej strony zapewnić możliwość organizacji danych w jednolite zbiory, z których system pozwoli tworzyć zestawienia, raporty i dokumenty adekwatne do rzeczywistych potrzeb odbiorców informacji.

[1] Autor jest ekspertem do spraw jakości danych w Centrum Systemów Informacyjnych Ochrony Zdrowia w Warszawie, pełnomocnikiem Ministra Zdrowia ds. otwartości danych publicznych.

[2] T.j. Dz.U. z 2017 r. poz. 1845 ze zm.

[3] Rozporządzenie Rady Ministrów z 12.4.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017 r. poz. 2247 ze zm.).

[4] Ustawa z 17.2.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2017 r. poz. 570 ze zm.).



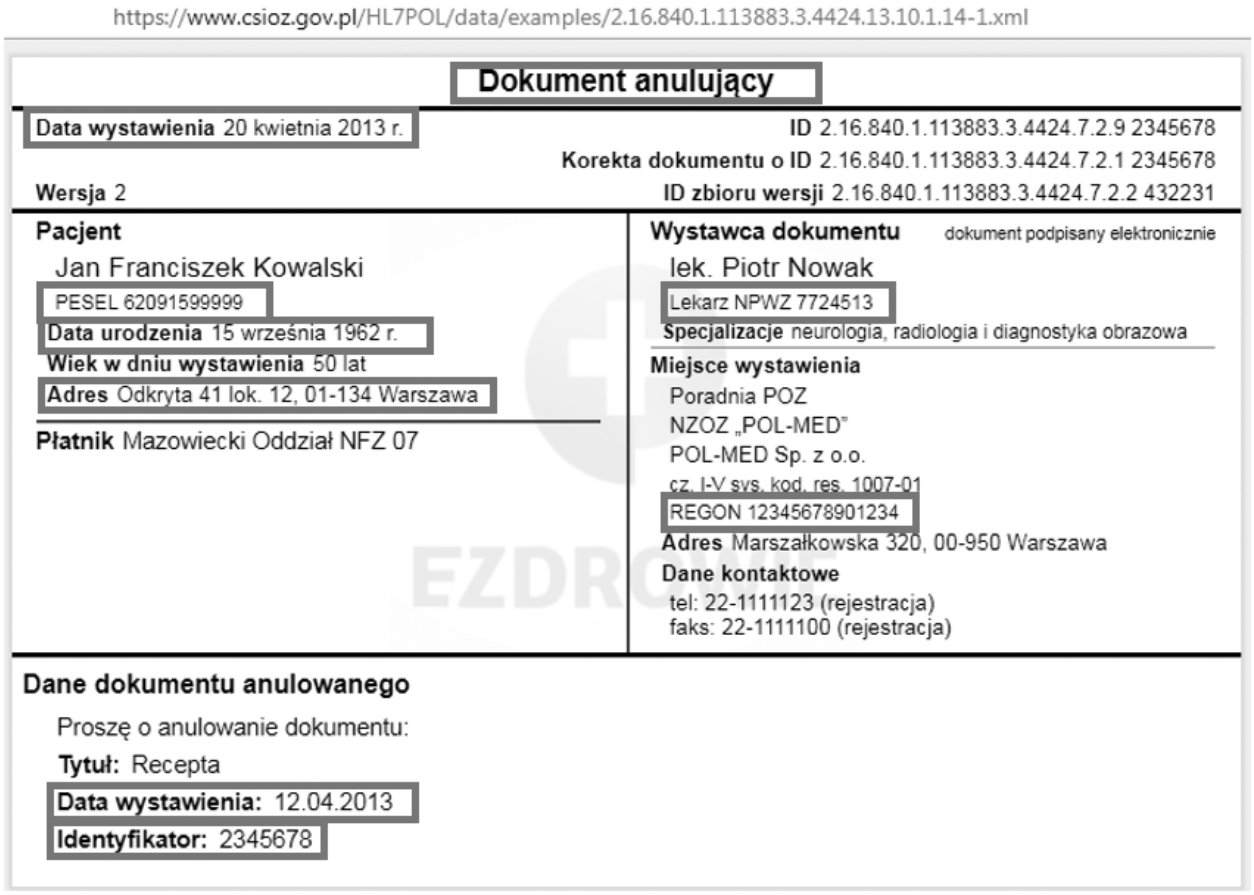
Rys. 1. Schemat systemu informacji w ochronie zdrowia[5] (opr. własne) przedstawia schematycznie (skrótowo) przepływy danych między jego własnymi i obcymi rejestrami oraz bazami danych

Na rys. 1 pokazano schemat (opr. własne), z którego wynika, że budowa systemu informacji w ochronie zdrowia jest przedsięwzięciem niezwykle skomplikowanym. Jest to podyktowane nie tylko rozległością terytorialną, różnorodnością elementów składowych, tym, że poszczególne elementy zarządzane są przez niezależne podmioty nawet pozornie niemające nic wspólnego z ochroną zdrowia, ale również tym, że budowa tego systemu jest działaniem niekończącym się, w trakcie którego pojawiają się (dołączane są) nowe systemy. Faktem jest, że niektóre zbiory danych, rejestry wchodzące w skład systemu informacji w ochronie zdrowia, opublikowane w portalu https://dane.gov.pl aktualizowane są w trybie codziennym, gdyż niemal każdego dnia pojawiają się lub są likwidowane gabinety lekarskie, apteki, ewentualnie zmienia się tylko miejsce działalności (adres), własność lub nazwa. W czasie tej niekończącej się rozbudowy powstają nowe relacje, nowe połączenia międzysystemowe, które mogą – jeśli proces ten nie będzie odpowiednio nadzorowany, prowadzić do naruszenia ochrony danych, ujawnienia informacji i dokumentów ustawowo podlegających ochronie. Ochronie podlegają nie tylko dane, ale przede wszystkim relacje między nimi, co właśnie ujawniają dokumenty. Skuteczna ochrona danych polega m.in. na zarządzaniu relacjami między danymi – ich tworzeniu lub zrywaniu. Należy jednak pamiętać, że można coś zobaczyć, ale nie da się tego procesu odwrócić („odzobaczyć") – informacji uwolnionej nie można z powrotem utajnić. Z tego powodu dokumenty przesyłane poza systemem powinny być zabezpieczane np. przez ich szyfrowanie lub silne hasło.

Dokumenty w ochronie zdrowia mają swoją specyfikę, niezależną od tego, czy występują w postaci papierowej czy elektronicznej. Ich zawartość informacyjną (dane i informacje) określają przepisy prawa. I tak np. pojęcie elektronicznej dokumentacji medycznej wprowadza ustawa o systemie informacji w ochronie zdrowia. Specyfika dokumentów w postaci elektronicznej wynika z ich budowy strukturalnej, umożliwiającej utworzenie dokumentu zgodnego ze wzorem zdefiniowanym w określonym, międzynarodowym standardzie (HL7 CDA), oraz maszynowe odczytanie danych zawartych w tym dokumencie i ich przetworzenie. W Polsce podmiotem powołanym do publikowania wzorów dokumentów medycznych jest Centrum Systemów Informacyjnych Ochrony Zdrowia[6].

[5] Ten sam system, lecz zobrazowany nieco inaczej (w mniejszym uproszczeniu, czyli bardziej szczegółowy – w papierowej wersji artykułu byłby całkowicie nieczytelny) został zamieszczony na stronie internetowej Centrum Systemów Informacyjnych Ochrony Zdrowia pod adresem: https://www.csioz.gov.pl/fileadmin/user_upload/Broszury/schemat_systemu_informacji_w_ochronie_zdrowia_56b0c687980a6.pdf. (dostęp z 11.1.2019 r.).

[6] Wzory dokumentów medycznych publikowane są na stronie: https://www.csioz.gov.pl/HL7POL/pl-cda-html-pl-PL/ (dostęp z 11.1.2019 r.).


https://www.csioz.gov.pl/HL7POL/data/examples/2.16.840.1.113883.3.4424.13.10.1.14-1.xml

Dokument anulujący

Data wystawienia 20 kwietnia 2013 r.

ID 2.16.840.1.113883.3.4424.7.2.9 2345678

Korekta dokumentu o ID 2.16.840.1.113883.3.4424.7.2.1 2345678

Wersja 2

ID zbioru wersji 2.16.840.1.113883.3.4424.7.2.2 432231

Pacjent

Jan Franciszek Kowalski

PESEL 62091599999

Data urodzenia 15 września 1962 r.

Wiek w dniu wystawienia 50 lat

Adres Odkryta 41 lok. 12, 01-134 Warszawa

Płatnik Mazowiecki Oddział NFZ 07

Wystawca dokumentu dokument podpisany elektronicznie

lek. Piotr Nowak

Lekarz NPWZ 7724513

Specjalizacje neurologia, radiologia i diagnostyka obrazowa

Miejsce wystawienia

Poradnia POZ
NZOZ „POL-MED"
POL-MED Sp. z o.o.
cz. I-V sys. kod. res. 1007-01
REGON 12345678901234
Adres Marszałkowska 320, 00-950 Warszawa

Dane kontaktowe

tel: 22-1111123 (rejestracja)
faks: 22-1111100 (rejestracja)

Dane dokumentu anulowanego

Proszę o anulowanie dokumentu:

Tytuł: Recepta

Data wystawienia: 12.04.2013

Identyfikator: 2345678

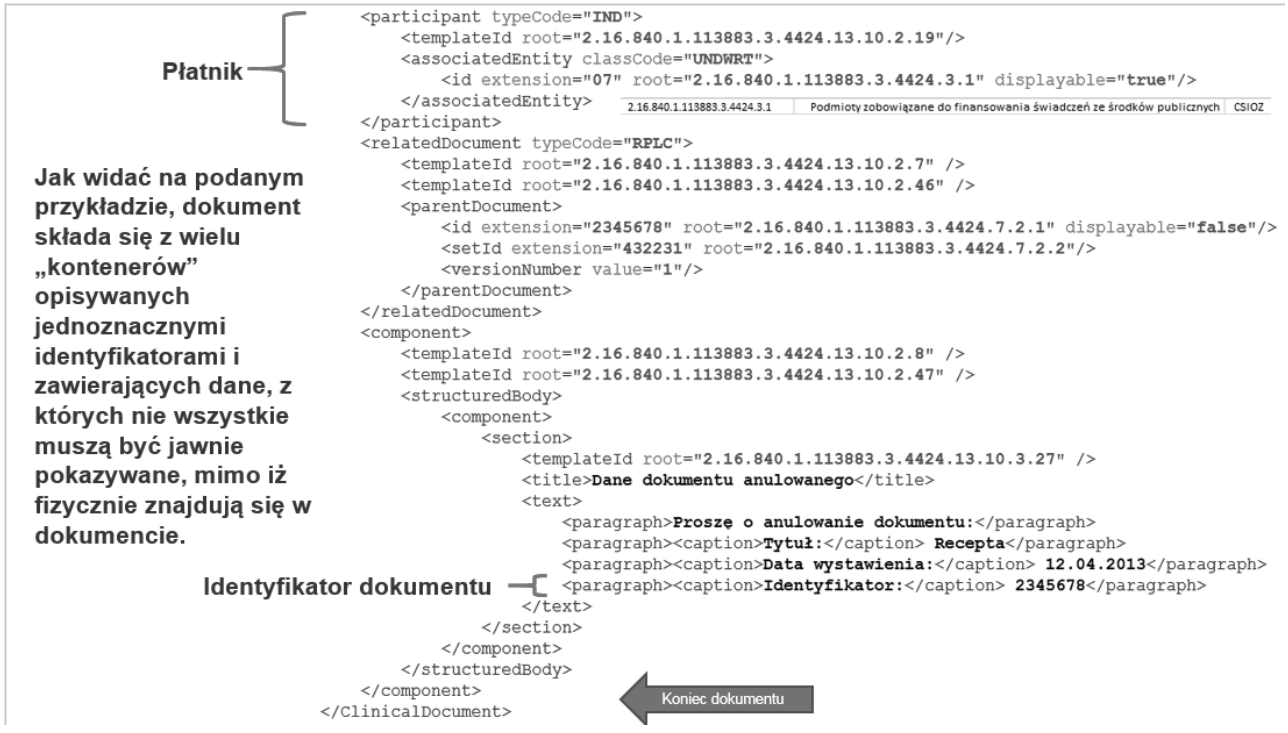
Rys. 2. Wygląd dokumentu anulującego receptę o numerze 2345678 z 12.4.2013 r.

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet href="CDA PL IG 1.2.xsl" type="text/xsl"?>
<ClinicalDocument
        xmlns="urn:hl7-org:v3"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:extPL="http://www.csioz.gov.pl/xsd/extPL/r1"
        xsi:type="extPL:ClinicalDocument">
    <!-- Anulowanie recepty na Enarenal -->
    <typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>
    <templateId root="2.16.840.1.113883.3.4424.13.10.1.1"/>
    <templateId root="2.16.840.1.113883.3.4424.13.10.1.14" extension="1.1.1"/>
    <id extension="2345678" root="2.16.840.1.113883.3.4424.7.2.9" displayable="true"/>
    <code code="51851-4" codeSystem="2.16.840.1.113883.6.1" codeSystemName="LOINC" displayName="Administrative note">
        <translation code="08.80" codeSystem="2.16.840.1.113883.3.4424.11.1.32" codeSystemName="KLAS_DOK_P1" displayName="Dokument
        anulujący"/>
    </code>
    <title>Dokument anulujący</title>
    <effectiveTime value="20130420"/>
    <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>
    <languageCode code="pl-PL"/>
    <setId extension="432231" root="2.16.840.1.113883.3.4424.7.2.2"/>
    <versionNumber value="2"/>
    <recordTarget>
        <templateId root="2.16.840.1.113883.3.4424.13.10.2.3"/>
        <patientRole>
            <id extension="12345" root="2.16.840.1.113883.3.4424.2.7.0.17.1" displayable="false"/>
            <id extension="62091599999" root="2.16.840.1.113883.3.4424.1.1.616" displayable="true"/>
            <addr>
                <city>Warszawa</city>
                <postalCode>01-134</postalCode>
                <streetName>Odkryta</streetName>
                <houseNumber>41</houseNumber>
                <unitID>12</unitID>
            </addr>
```

Początek dokumentu

Wewnętrzna struktura dokumentu pokazanego na poprzednim slajdzie

Rys. 3. Fragment kodu dokumentu anulującego receptę – widoczny PESEL – identyfikator pacjenta



Rys. 4. Dalszy fragment kodu dokumentu anulującego receptę – widoczny identyfikator dokumentu, który ma być anulowany

Na rys. 2 pokazano pochodzący ze wskazanej w poprzednim zdaniu strony dokument anulujący wystawioną receptę, której numer i datę wystawienia, wystawcę oraz pacjenta i wiele innych danych jednoznacznie można odczytać, gdyż wizualizacja przeznaczona jest dla człowieka. Tak wygląda wydruk dokumentu anulującego wystawioną receptę – bez względu na to, czy będzie on wydrukowany na papierze, czy zostanie utworzony jako plik w formacie pdf. Na rys. 3 pokazano fragment tego samego dokumentu, ale jako kodu odczytywalnego przez system informatyczny, interpretujący odpowiednio dane. Niektóre z danych zaznaczono ramkami, by ułatwić Czytelnikowi porównanie danych przedstawionych na rys. 3 z danymi na rys. 2. Na rys. 4 pokazano dalszą część kodu tego samego dokumentu ze wskazaniem miejsc dotyczących konkretnych osób związanych z dokumentem, a więc jego wystawcy – lekarza – i pacjenta. W tym momencie należy wskazać na fakt, że taki sposób zapisu danych – w postaci elektronicznej ze znacznikami otaczającymi dane – pozwala tworzyć różnego rodzaju relacje (powiązania) między odrębnymi dokumentami. Te relacje występują pomiędzy jednoznacznymi identyfikatorami każdego z dokumentów. Najogólniej bowiem rzecz ujmując, każdy obiekt w systemie musi posiadać swój jednoznaczny identyfikator, pozwalający zidentyfikować go w całym zbiorze obiektów tego samego rodzaju. Przykładowo dla pacjenta będzie to numer PESEL (jako identyfikator globalny w jakimkolwiek zbiorze zawierającym dane osób fizycznych), dla lekarza – numer prawa wykonywania zawodu (NPWZ), niezależnie od numeru PESEL lekarza, który też może być pacjentem. Właściwe identyfikatory używane są bowiem zależnie od kontekstu.

Jeśli więc przyjmiemy wspomnianą wyżej zasadę, że wszystkie obiekty (osoby fizyczne, podmioty lecznicze, dokumenty, choroby, procedury medyczne, leki, poszczególne dane itd.) mają jednoznacznie identyfikujące je identyfikatory, wtedy mamy już możliwość tworzenia zarządzalnych relacji między tymi obiektami.

Naturalną konsekwencją muszą być zasady zarządzania tymi relacjami, co *de facto* oznacza zarządzanie uprawnieniami dostępu do danych i dokumentów. Poziomy tych uprawnień (zakres dostępu, możliwość odczytu lub odczytu i zapisu, komentowanie, dodawanie metadanych itp.) muszą być uwarunkowane celowościowo.

Uwarunkowania celowościowe

Podstawowym celem działania systemu ochrony zdrowia jest ochrona zdrowia i życia osób fizycznych. Na pierwszym miejscu jest pacjent, a nie opisujące go dane. Osiągnięcie tego celu wymaga gromadzenia i przetwarzania danych opisujących stan zdrowia pacjenta i utrwalania tych danych w dokumentacji medycznej do przyszłego wykorzystania (cele naukowe, statystyczne, ekonomiczne itp., ale z zachowaniem poufności).

Gromadzone dane i dokumenty muszą być dostępne dla pracowników medycznych zaangażowanych w proces leczenia – i to niezależnie od lokalizacji miejsca udzielania świadczenia medycznego, gdyż pacjent może leczyć się w miejscach nawet bardzo terytorialnie odległych.

Powyższe implikuje potrzebę stosowania takich sposobów zapisu danych (czasowy) i dokumentów (trwały), by – niezależnie od stosowanego w danym podmiocie systemu – dane i dokumenty dało się nie tylko jednoznacznie odczytać, ale także upewnić się co do ich autentyczności – wszystko to w czasie długości trwania życia człowieka, czyli w perspektywie kilku dziesiątków lat. Jest to ogromne wyzwanie, zwłaszcza jeżeli chodzi o okres, gdy dane były zapisywane jedynie w dokumentach papierowych. Co prawda ich wygląd w zasadzie się nie zmieniał, jednak występowały problemy związane z niekompletnością, nieczytelnością pisma odręcznego lekarza i związane z tym zagrożenia wydania niewłaściwego leku lub potrzeby powrotu do lekarza w celu uczytelnienia wpisu. Ponadto tworzenie jakichkolwiek relacji między dokumentami było, jeśli nie niemożliwe, to znacząco utrudnione. Dokumenty gromadzone w teczkach, segregatorach, łączone spinaczami i zszywaczami nie nadają się do analiz statystycznych, gdyż pracochłonność związana z ich obróbką jest nieadekwatnie wysoka w stosunku do wyników przetwarzania, nie mówiąc o całkowicie realnych zagrożeniach poufności osobowych danych medycznych.

Jeśli chodzi o dane, informacje i dokumenty w postaci elektronicznej rzecz ma się zdecydowanie lepiej. Możliwe jest bowiem (w sensie technicznym) tworzenie systemów, w których jest zapewniona rozliczalność działania osób posiadających uprawnienia do ich wykorzystywania i to na różnych poziomach uprawnień, a także zapewniona jest poufność danych medycznych pacjentów. Tajemnica lekarska przestaje być całkowicie iluzoryczna, to system zapewnia bowiem dostęp osoby uprawnionej z jednoczesną rejestracją faktu udostępnienia (analogicznie, jak to jest w elektronicznych systemach zarządzania dokumentami zgodnymi z rozporządzeniem w sprawie instrukcji kancelaryjnej[7]). W systemach takich dane medyczne pacjentów są dostępne jedynie dla uprawnionych pracowników, posiadających dostęp warunkowany zarówno prawami dostępu, nadanymi przez kierownika podmiotu, jak i posiadaniem odpowiednich narzędzi – elektronicznego certyfikatu/klucza sprzętowego i hasła. Nie jest fizycznie możliwe zalogowanie się do systemu bez posiadania ww. narzędzi. Należy też uświadomić sobie fakt, że w momencie cofnięcia uprawnień dostępu do zasobów nawet posiadanie klucza sprzętowego i hasła nie pozwoli na zalogowanie się w systemie. Gdyby bowiem doszło do sytuacji, w której lekarz np. zgubi elektroniczną kartę z certyfikatem, wystarczy telefon do administratora – i ten może zablokować dostęp do zagrożonego konta do momentu wygenerowania nowego certyfikatu i ustalenia nowego hasła przez lekarza.

Z kolei pacjent może w każdej chwili uzyskać wszystkie dotyczące go dokumenty medyczne – zabezpieczone elektronicznie (zaszyfrowane, elektronicznie podpisane – są różne możliwości ich pobrania z systemu i przesłania do miejsca docelowego wykorzystania).

Ważnym, choć wydaje się, że ciągle jeszcze niedocenianym elementem każdego lokalnego lub – lepiej – regionalnego systemu przechowującego dokumenty (nie dane, ale właśnie dokumenty, które w sobie mają zapisane dane wraz z opisującymi je metadanymi) są repozytoria oraz archiwa głębokie.

Między repozytorium a archiwum głębokim istnieje bufor, który zabezpiecza je całkowicie przed nieuprawnionym wejściem, przeszukiwaniem czy pobraniem dokumentów. Repozytorium pozwala na przechowywanie plików (dokumentów) przez zadany okres (np. dwa lata). Jednocześnie pliki w trybie codziennym przed północą przesyłane są do archiwum głębokiego, gdzie mogą być składowane dziesiątki lat. Pliki starsze niż wymagany okres przechowywania są automatycznie usuwane z repozytorium. Nie ma potrzeby dłuższego ich przechowywania, gdyż pociągałoby to za sobą niepotrzebne rozbudowywanie owego repozytorium o kolejne dyski (całkowicie zbędne koszty materiałowe, koszty konserwacji). Pliki zawarte w repozytorium, jak już wcześniej wspomniano, są kopiowane do archiwum głębokiego tego samego dnia, w którym zostały utworzone. Jeśli zaistnieje taka potrzeba, mogą zostać na żądanie pobrane z archiwum na normalnych zasadach: żądanie osoby uprawnionej oraz rejestracja faktu wydania dokumentu z archiwum. Oczywiście wydana będzie jedynie kopia zero-jedynkowo zgodna z plikiem zapisanym w archiwum. Dokumenty zapisane w archiwum nigdy go nie opuszczają.

Inaczej rzecz ma się z repozytorium. Dokumenty zapisane w repozytorium w czasie tworzenia – dopóki nie zostaną ukończone (czyli elektronicznie podpisane), dopóty są dokumentami roboczymi, operacyjnymi dostępnymi do edycji bezpośrednio, on-line dla lekarza i uprawnionych osób mogących dokonywać wpisów we właściwych polach dokumentu. Dokument może mieć np. wygląd formularza zawierającego pola, w których powinny znaleźć się określone dane. Formularz jest jednak – jak to już pokazano na przykładzie dokumentu anulującego receptę – jedynie pewną wizualizacją ułatwiającą stwierdzenie, czy wszystkie wymagane dane zostały już zgromadzone. Jednak dane nie są zapisane w formularzu, a w pliku XML w kontenerach opisanych właściwymi znacznikami. Taka konstrukcja dokumentów (ściśle zdefiniowana i uporządkowana struktura właściwa dla

[7] Rozporządzenie Prezesa Rady Ministrów z 18.1.2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. Nr 14, poz. 67 ze zm.).

każdego wzoru) pozwala na operacje całkowicie niemożliwe do wykonania w odniesieniu do dokumentów papierowych. Umożliwia mianowicie selektywne wybieranie danych do badań naukowych i sprawozdań statystycznych bez naruszania poufności danych medycznych, czyli w oderwaniu od danych osobowych pacjentów. Przenosi to bezpieczeństwo osobowych danych medycznych na całkowicie inny poziom[8].

Z kolei archiwum głębokie to takie archiwum elektroniczne, które służy do składowania dokumentów medycznych (generalnie plików w różnych formatach, także obrazów, filmów, plików tekstowych i multimedialnych) w środowisku zapewniającym kontrolę nośników, stanu dysków, zapisów danych ze stosowną nadmiarowością, tak by w razie uszkodzenia, utraty pojedynczych bitów możliwe było odtworzenie zapisanego dokumentu bez zniekształceń niesionej treści. Szczegółowe opisanie zastosowanych w tym celu mechanizmów znacznie przekraczałoby ramy niniejszego artykułu. Istotne jest jednak to, że istnieją już obecnie krajowe rozwiązania techniczne, możliwe do praktycznego zastosowania i znacznie tańsze niż technologicznie już przestarzałe powszechnie stosowane rozwiązania (nie należy mylić archiwum wieczystego z systemem backupowym, służącym do odtwarzania danych po awariach systemu).

Ochrona danych osobowych medycznych obejmuje różne obszary, takie jak:
- ochrona przed nieuprawnionym pozyskaniem czy wglądem;
- ochrona przed zafałszowaniem;
- ochrona przed uszkodzeniem, zniszczeniem;
- ochrona przed utratą.

Wiele zależy od postaci nośnika, na którym zapisywane są informacje/dane (postać dokumentu). Jak już wcześniej wspomniano, ochrona danych i dokumentów w postaci elektronicznej, z uwagi na rozliczalność uzyskaną dzięki silnym mechanizmom weryfikacji tożsamości użytkownika systemu, jest zdecydowanie silniejsza. Ważniejsza jednak od ochrony danych jest ochrona osób fizycznych, których te dane dotyczą, co niejako jest wskazane w samym tytule aktu prawnego odnoszącego się do tej problematyki, czyli rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)[9].

Należy także pamiętać, że przy tworzeniu i rozbudowie systemu informacji w ochronie zdrowia należy zachować pewne warunki, takie jak:
- poprawa danych w rejestrach (słownikowanie, usuwanie niezgodności, uzupełnianie braków);
- przy tworzeniu nowych systemów stosowanie zasad „*privacy by design*", a przy nadawaniu uprawnień dostępu do danych i dokumentów zasady „*privacy by default*";
- wprowadzanie identyfikatorów elektronicznych, certyfikatów dostępowych i certyfikatów służących do składania podpisów.

Ostatni z ww. warunków może być realizowany w różny sposób. Jakiekolwiek prawne regulowanie koniecznych do zastosowania środków technicznych byłoby bowiem pozbawione sensu z uwagi na stale zmieniającą się i doskonaloną technologię (łącznie z możliwością zastosowania silnych biometrii), która umożliwia z jednej strony coraz prostsze, a z drugiej coraz pewniejsze sposoby wiarygodnego „przedstawienia się" systemowi teleinformatycznemu. Wykonywanie jakiejś czynności po zalogowaniu się do systemu skutkuje automatycznym zapisem czynności zalogowanego użytkownika, który – oprócz różnych danych opisujących szczegółowo jego uprawnienia, stanowisko, imię i nazwisko, kontekst, w jakim działa (ten sam pracownik w systemie może mieć różne uprawnienia w zależności od kontekstu, roli, w jakiej występuje, i od jednostki organizacyjnej, w ramach której w danym momencie pracuje) – jest zawsze identyfikowalny dzięki posiadaniu jednoznacznego identyfikatora, jakim jest numer PESEL. Podobnie podmiot, w ramach którego ów użytkownik wykonuje swoje zadania, musi być jednoznacznie identyfikowany – przez numer REGON. Sprawy jednoznacznej identyfikacji oraz przenaszalności danych i dokumentów między systemami uregulowane zostały rozporządzeniem w sprawie Krajowych Ram Interoperacyjności. Warunki osiągania interoperacyjności opisane w powołanym akcie częstokroć nie są jednak znane i przestrzegane przez podmioty inne niż te, których dotyczy ustawa o informatyzacji. Podmioty te traktują zasady interoperacyjności jako zbędne obciążenie czy ograniczenie ich swobody oraz źródło zbędnych kosztów dostosowania ich systemów do bliżej nieokreślonych systemów podmiotów realizujących zadania publiczne. Jest to jednak dość krótkowzroczne podejście, gdyż tak jak np. systemy niepublicznych zakładów ochrony zdrowia zasilać mogą danymi system informacji w ochronie zdrowia, tak systemy zarządzane przez podmioty realizujące zadania publiczne zasilać mogą systemy podmiotów niepublicznych. Celowi temu służy program otwierania danych publicznych. W konsekwencji powstał portal (pierwotnie danepubliczne.gov.pl, aktualnie dane.gov.pl), na którym znajdują się zarówno dane, jak i aplikacje służące do bardzo różnych celów – czyli takie, które mogą być wykorzystywane nie tylko w celu, dla którego zostały zebrane, ale także w jakimkolwiek innym.

Związek wspomnianego portalu z systemami ochrony zdrowia jest dość istotny – można w nim odszukać poprawnie zapisane zbiory adresowe (zbiór „Dane adresowe gmin") oraz aplikację do sprawdzania adresu uniwersalnego

[8] *K. Anders* i in., Ochrona danych osobowych medycznych, wyd. 2, Warszawa 2018, *passim*.

[9] Dz.Urz. UE L 119, s. 1; dalej jako: RODO.

(http:/ itia.pl/adres). Podmioty lecznicze, samorząd lekarski i pielęgniarski, farmaceuci, wprowadzając do prowadzonych i zarządzanych przez siebie systemów jakikolwiek adres fizyczny (w terenie), powinni za pomocą wspomnianej wyżej aplikacji zweryfikować adres, który zamierzają wprowadzić np. do wniosku rejestracyjnego.

W czasie wprowadzania adresu (ściślej, wyboru poszczególnych składowych adresu z list wyboru) można ustalić poprawną konstrukcję adresu i zobaczyć punkt adresowy na wygenerowanej mapce.

W tym konkretnym przypadku dane źródłowe, pochodzące z gmin zasilają rejestry centralne prowadzone przez GUS (TERYT – rejestr podziału terytorialnego kraju) oraz GUGiK (Państwowy Rejestr Granic). Aplikacja do sprawdzania adresu uniwersalnego wiąże ze sobą dane obu wyżej wspomnianych rejestrów. Dzięki temu, że w danych PRG osadzone są kody terytorialne (oraz dodatkowo kody pocztowe PNA), możliwe jest wzajemne ich powiązanie i wygenerowanie adresu uniwersalnego, łączącego w sobie wszystkie elementy niezbędne zarówno do wygenerowania adresu uniwersalnego, jak i poprawnego adresu fizycznego rzeczywiście istniejącego obiektu. W ochronie zdrowia poprawność wskazania adresu może decydować o tym, czy ekipa pogotowia ratunkowego dojedzie do wskazanego miejsca jeszcze za życia osoby poszkodowanej.

Rys. 5. Nazwa ulicy dla tego samego punktu adresowego zapisana w systemach niezależnych od siebie

Na rys. 5 pokazano przykład punktu adresowego, dla którego nazwa ulicy ma wprawdzie różne brzmienie w powołanych wyżej rejestrach centralnych (co jest oczywistym błędem urzędników, gdyż źródłem nazwy jest ta sama rada gminy i nazwa jednoznacznie zapisana jest w uchwale), ale dzięki temu, że w obu wersjach nazwy występuje wspólny element „Łukasińskiego", system potrafi wskazać na mapie poszukiwany punkt adresowy. W rzeczywistości istnieją różne, inne jeszcze przypadki zakłóceń, takie jak np. występowanie w tej samej miejscowości dwóch różnych, oddalonych od siebie ulic (np. ul. Wilanowska w Warszawie), które jednak – dzięki odmiennemu kodowi pocztowemu – także można od siebie odróżnić. Niemniej problem niespójności adresów jest problemem stałym i jedynie upowszechnianie wiedzy o zagrożeniach stwarzanych przez niespójne dane czy ich brak w systemach teleinformatycznych oraz rejestrach może spowodować zwiększoną uwagę przy wprowadzaniu danych do rejestrów systemów informacyjnych mających interoperacyjnie współdziałać ze sobą.

Wdrożenie interoperacyjnych i bezpiecznych e-usług wymaga zdecydowanego uporządkowania zawartości rejestrów stosowanych w administracji publicznej, w szczególności rejestrów centralnych zarówno w zakresie ich kompletności, jak i zawartości informacyjnej. Należy doprowadzić do zmiany przepisów prawa utrudniających lub uniemożliwiających uspójnienie danych oraz wymuszających ich powielanie (te same dane w tym samym czasie nie mogą mieć w różnych rejestrach różnej wartości – aktualnie jest to niemal norma). Obecnie administrator systemu widzi błędy, ale niedostosowane do realiów prawo nie pozwala mu ich usunąć. Z kolei

administrator danych lub ich właściciel mógłby usunąć błędy, ale ich nie dostrzega, a najczęściej nie ma także świadomości ich istnienia (mimo że sam dane do rejestrów wprowadza). Dane rejestrowe powinny być wiązane z jednoznacznymi identyfikatorami – zgodnie z Krajowymi Ramami Interoperacyjności. Wiązałoby się to jednak ze zmianą zakresu podmiotowego ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne – i także jej nazwy. Znowelizowana ustawa o informatyzacji musiałaby bowiem objąć także rejestry podmiotów niepublicznych – w tym rejestry prowadzone przez samorządy zawodowe, jeśli stanowią one źródło danych dla rejestrów centralnych, jak ma to np. miejsce w przypadku Rejestru Podmiotów Wykonujących Działalność Leczniczą[10]. W rejestrze tym ujęte są nie tylko podmioty, dla których organem rejestrowym jest wojewoda, ale także indywidualne i grupowe praktyki lekarzy i lekarzy dentystów oraz indywidualne i grupowe praktyki pielęgniarek i położnych. Z jednej strony ustawa z 15.4.2011 r. o działalności leczniczej[11] w art. 106 wskazuje organy rejestrowe, a z drugiej traktuje je nierówno, dyskryminacyjnie, gdyż nakładając obowiązki, nie zapewnia narzędzi realizacji zadań (jak np. nie nadaje funkcjonalności podmiotu publicznego okręgowym izbom lekarskim i pielęgniarskim pozwalającym we właściwy sposób wykorzystywać Elektroniczne Skrzynki Podawcze na platformie ePUAP). Naruszona jest zasada równoważności w zakresie nadawania praw i nakładania obowiązków. Organ rejestrowy, jakim jest wojewoda, funkcjonalność taką uzyska, ponieważ urząd wojewódzki jest podmiotem realizującym zadania publiczne, a okręgowe (i naczelne) izby samorządów zawodowych – mimo że ustawowo zmuszone zostały do prowadzenia rejestrów, funkcjonalności takiej nie uzyskały. Dyskryminacja i nierówne traktowanie różnych podmiotów, mimo iż niektóre z nich tworzone są z mocy ustawy i ewidentnie wykonują zadania społecznie potrzebne, widoczne są doskonale np. w wykazie Elektronicznych Skrzynek Podawczych, w którym jedynie Naczelna Izba Lekarska oraz trzy Okręgowe Izby Lekarskie uzyskały funkcjonalność podmiotu publicznego, podobnie jak kilka niepublicznych zakładów opieki zdrowotnej, a kilkadziesiąt innych organów rejestrowych – mimo że składały wnioski o nadanie funkcjonalności podmiotu publicznego – już nie.

Sytuacja taka jest ewidentną przeszkodą w tworzeniu bezpiecznego i spójnego elektronicznego środowiska przetwarzania danych i przesyłania dokumentów w postaci elektronicznej.

Podsumowanie

Stworzenie bezpiecznego, sprawnego środowiska przetwarzania danych i wykorzystywania dokumentów w postaci elektronicznej wymaga spełnienia pewnych warunków dotyczących spójnego i niedyskryminacyjnego stosowania prawa, zachowania równowagi w nakładaniu obowiązków i przyznawania praw, jak też spełnienia całkowicie realnych warunków technicznych, związanych z zapewnieniem interoperacyjności systemów wszelkich podmiotów zasilających danymi rejestry współpracujące z systemem informacji w ochronie zdrowia, lub do niego należącymi. Bez spełnienia powyższych warunków jego budowa będzie nadmiernie kosztowna, a sam system ciągle będzie generował czy ujawniał błędy różnego rodzaju i nie będzie w pełni realizował oczekiwań względem jego funkcjonalności. Należy sobie uświadomić, że sprawny system informacji w ochronie zdrowia umożliwi nie tylko tworzenie e-usług, ale także realizację programu otwierania danych publicznych[12] – a to z kolei ma znaczenie dla podmiotów świadczących usługi medyczne.

[10] Zob. https://rpwdl.csioz.gov.pl (dostęp z 11.1.2019 r.).
[11] T.j. Dz.U. z 2018 r. poz. 160 ze zm.
[12] Uchwała Nr 107/2016 Rady Ministrów z 20.9.2016 r. w sprawie ustanowienia „Programu otwierania danych publicznych", https://mc.bip.gov.pl/programy-realizowane-w-mc/programu-otwierania-danych-publicznych.html (dostęp z 11.1.2019 r.).

Słowa kluczowe: ochrona danych medycznych, otwieranie danych, interoperacyjność, rejestry publiczne, informacja w ochronie zdrowia, dokumenty medyczne, repozytorium, archiwum głębokie.

Computerization of resources of entities running medical activity. Interoperability and data protection – how does it work?

The aim of the present study is to point out specification of a very complex system of information in health protection within which there is processing of data. Firstly, the issue concerns data of which common and unconditional sharing is a social benefit and the data may be used for different purposes, not necessarily for the one that system has been built. Secondly, this data has to be protected because it is personal data, including data of special category.

Keywords: protection of medical data, opening data, interoperability, public register, information in health protection, medical documents, repository, deep archive.

WYMOGI EDYTORSKIE:

- język publikacji: polski, angielski, niemiecki, rosyjski;
- edytor tekstu Word (format .doc lub .docx);
- styl czcionki: Times New Roman;
- wielkość czcionki: tekst główny – 12 pkt, przypis – 10 pkt;
- interlinia: 1,5 wiersza (w przypadku przypisów – 1 wiersz);
- objętość artykułu: do 30 000 tys. znaków ze spacjami;
- marginesy: standardowe – wszystkie 2,5 cm;
- przypisy dolne: odsyłaczami przypisów powinny być cyfry arabskie; odsyłacz należy umieścić bezpośrednio po fragmencie, do którego odnosi się przypis (przed kropką kończącą zdanie);
- należy dołączyć słowa kluczowe w języku polskim i angielskim;
- tytuł powinien być napisany czcionką Times New Roman 14 pkt (czcionka pogrubiona);
- tekst powinien składać się z następujących części: lid (streszczenie ok. 1500 znaków ze spacjami), uwagi wstępne, rozwinięcie (z podziałem na zatytułowane części), podsumowanie;
- do artykułu należy załączyć także lid (streszczenie) w języku angielskim (ok. 1500 znaków ze spacjami);
- śródtytuły nie powinny być numerowane, lecz pogrubione;
- należy dołączyć notę biograficzną (ok. 800 znaków ze spacjami);
- prosimy o wskazanie afiliacji.

Powoływane w przypisach pozycje bibliograficzne prosimy pisać według wzoru:

Inicjał. Nazwisko, Tytuł, ew. numer wydania, tom, część itp., miejsce i rok wydania, a następnie cytowane strony skrótem „s.", np.: *J. Kowalski*, Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku kolejnego powołania się **bezpośrednio** na cytowaną pozycję:

Ibidem, s. 15–16.

Powołanie kolejny raz, gdy cytujemy tylko jedną pozycję danego autora:

J. Kowalski, *op. cit*., s. 29–20.

Kolejne powołanie, gdy cytuje się kilka pozycji danego autora, zawiera pierwsze wyrazy tytułu, np.:

J. Kowalski, Jak pisać..., s. 28–29.

W przypadku **prac pod redakcją**, jeśli powoływana publikacja stanowi część całości:

P. Igrek, Cytowanie, [w:] *J. Kowalski* (red.), Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku publikacji w czasopismach tytuł czasopisma zastępuje nazwę wydawnictwa, po nim następuje rok (rocznik), przecinek, następnie numer (nr) w ramach rocznika ewentualnie także numer od początku wydawania pisma i numer strony:

J. Kowalski, Jak pisać przypisy?, Wiadomości Tekściarskie 2006, Nr 28 (236), s. 7.

Kilka kwestii specjalistycznych:

1. Oczekiwane oznaczenie ustawy wygląda następująco: Dz.U. z 2006 r. Nr 28, poz. 456.
2. Publikator prosimy podawać jedynie przy pierwszym przywołaniu aktu prawnego. Wówczas nazwę aktu i datę (miesiąc słownie) podajemy w tekście głównym (np. ustawa z 13.4.2003 r. o zasadach pisania artykułów), w przypisie zaś publikator (np. t.j. Dz.U. z 2006 r. Nr 28, poz. 456).
3. Zapisując artykuł, ustęp, punkt aktu prawnego, skrótów nie oddzielamy przecinkami, tak więc: art. 28 ust. 59 pkt (bez kropki!) 36, a nie: art. 28, ust. 59, pkt. 36.
4. W przypadku orzeczeń sądowych prosimy o zastosowanie następujących oznaczeń: Wyrok SN z 11.5.2011 r., I CA 123/11, OSNCP 2011, Nr 8, poz. 34. Nazwę orzeczenia i jego datę prosimy podać w tekście głównym (np. wyrok SN z 11.5.2011 r.), natomiast w przypisie publikator (I CA 123/11, OSNCP 2011, Nr 8, poz. 34).

Harmonogram publikacji:

Nr 1 – teksty do końca stycznia, druk luty/marzec
Nr 2 – teksty do końca kwietnia, druk maj/czerwiec
Nr 3 – teksty do końca lipca, druk sierpień/wrzesień
Nr 4 – teksty do końca października, druk listopad/grudzień

Osoba do kontaktu: dr *Aleksandra Klich*, e-mail: pme@beck.pl

EDITORIAL REQUIREMENTS:

- language of publication: Polish, English, German, Russian;
- text editor MS Word (.doc or .docx);
- font style: Times New Roman;
- font size: main text – 12 pts, footnote – 10 pts;
- line spacing: 1.5 line (for footnotes – 1 row);
- volume of the article: up to 30,000 characters with spaces;
- margins: standard – all 2.5 cm;
- footnotes: cross-referenced footnotes should be Arabic numerals; reference should be placed immediately after the passage to which the footnote regards (before the full stop ending a sentence);
- article must be attached with key words in Polish and English;
- the title should be written in Times New Roman 14 pts (bold);
- text should consist of following parts: lead (summary, around 1500 characters with spaces), initial comments, amplification (with a division into parts with titles), summation;
- article should also be attached with a lead (summary) in English (around 1500 characters with spaces);
- intertitles should not be numbered, but bold;
- article must be attached with a biographical note (approx. 800 characters including spaces);
- please indicate affiliation.

The referenced sources should adhere to the following style:

Initial(s). Last name, Title, edition number if applicable, volume, part, etc., place and year of publication, followed by the page(s) referred to with the 'p. (pp.)' abbreviation, e.g.: *J. Kowalski*, How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For subsequent reference made **directly** to the cited item:

Ibidem, p. 15–16.

Further reference, when several positions by a given author are being cited, include the first words of the title, e.g.:

J. Kowalski, How to..., p. 28–29.

For edited volumes, when the publication referenced forms a part of the whole:

P. Igrek, Citing, [in:] *J. Kowalski* (ed.), How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For publications in periodicals, the title of the periodical replaces the name of the publisher, followed by the year, comma, then the number (No.) within the year, possibly the consecutive number and page numbers:

J. Kowalski, How to do references?, Editorial news 2006, No. 28 (236) p. 7.

A few technical issues:

a. Expected indication of a legal act goes as follows: Journal of Laws of 2006, No. 28, item 456. The publishing body should only be provided when referring to the act for the first time. Then the name and date of the act (month – in words) shall be given in the body of the text (e.g. The Act of 13 April on the rules of writing articles), and the publishing body shall be given in the footnote (e.g. Journal of Laws of 2006, No. 28, item 456).
b. When writing article, paragraph, point of a legal act, abbreviations should not be separated by commas, that is: art. 28 par. 59 point (no full stop!) 36, not: art. 28, par. 59, pt. 36).
c. For court judgements, please use the following indications: Judgement of the Supreme Court of 11.5.2011, I CA 123/11, OSNCP 2011, No. 8, item 34. Mind that the appelative of the judgement and its date should be indicated in the main text (e.g. Judgement of the Supreme Court of 11.5.2011), and the publishing body in the footnote (I CA 123/11, OSNCP 2011, No. 8, item 34).

Publication schedule (deadlines):

No. 1 – submitting manuscripts – end of January (print – February/March)
No. 2 – submitting manuscripts – end of April (print – May/June)
No. 3 – submitting manuscripts – end of July (print – August/September)
No. 4 – submitting manuscripts – end of October (print – November/December)

Contact Person: *Aleksandra Klich* PhD, e-mail: pme@beck.pl