Marek Długozima

DOI: 10.23734/23.18.036

Wydatki na wdrożenie nowych regulacji prawnych w zakresie ochrony danych osobowych na przykładzie wybranej gminy

Streszczenie

W związku z obowiązkiem bezpośredniego stosowania przez państwa członkowskie Unii Europejskiej rozporządzeń Parlamentu Europejskiego i Rady podmioty przetwarzające dane osobowe są zobowiązane, od maja 2018 roku, przestrzegać nowych standardów określonych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). W artykule oszacowano koszty bezpośrednie niezbędnych działań dostosowawczych i nakłady na infrastrukturę eksploatowaną przez badaną gminę, głównie informatyczną.

Słowa kluczowe

ochrona danych osobowych, RODO, koszty, rachunek kosztów, jednostki samorządu terytorialnego

Wprowadzenie

W związku z obowiązkiem bezpośredniego stosowania przez państwa członkowskie Unii Europejskiej rozporządzeń Parlamentu Europejskiego i Rady podmioty przetwarzające dane osobowe są zobowiązane, od maja 2018 roku, przestrzegać nowych standardów określonych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[1] (RODO). Przedmiotem regulacji RODO, który jednocześnie będzie wskazywał obszary ponoszenia wydatków na działania dostosowawcze, są:

- zasady przetwarzania danych osobowych, w tym tzw. danych wrażliwych (np. o stanie zdrowia, poglądach politycznych, pochodzeniu rasowym, karach itp.)[2];

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016).

[2] Kategorie danych szczególnych określono w art. 10 RODO.

- prawa osób fizycznych, której dane dotyczą;
- zasady informowania i komunikowania się Administratora Danych Osobowych (ADO) z osobami, których dane przetwarza;
- obowiązki ADO i podmiotów przetwarzających dane osobowe głównie w zakresie ochrony prywatności osób fizycznych, w tym szacowanie ryzyka naruszenia ochrony danych osobowych i dobór wystarczających organizacyjnych i technicznych środków ochrony, powoływanie Inspektora Ochrony Danych Osobowych (IOD), certyfikacja podmiotów przetwarzających dane osobowe, przygotowanie i przestrzeganie kodeksów postępowania;
- przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych – obszar, który raczej nie występuje w gminach;
- właściwości, zadania, uprawnienia i współpracę organów nadzorczych. W Polsce został powołany tylko jeden organ nadzorczy i jego funkcję ma pełnić Prezes Urzędu Ochrony Danych Osobowych, który będzie współpracował z Europejską Radą Ochrony Danych;
- środki ochrony prawnej, odpowiedzialność i sankcje dla organu nadzorczego, ADO i podmiotu przetwarzającego;
- przypadki szczególne przetwarzania danych osobowych, np. w poszczególnych krajach członkowskich, dla poszczególnych grup danych osobowych, np. pracowniczych, do realizacji niektórych celów, np. naukowych.

Analiza obowiązków i zasad, określonych w RODO, które od maja 2018 roku ma stosować gmina, wskazuje na konieczność zaangażowania znacznych zasobów i podjęcia wielu działań, aby dostosować aktualnie stosowane rozwiązania do nowych standardów.

Stąd też w artykule podjęto próbą oszacowania niezbędnych wydatków na wdrożenie nowych wymagań. Wydatki te z pewnością w części będą generowały koszty funkcjonowania urzędu obsługującego organ wykonawczy gminy, a w części nakłady na eksploatowaną infrastrukturę.

Na potrzeby tego artykułu zbadano: akty prawne regulujące sferę ochrony danych osobowych przed i po 25 marca 2018 roku, politykę bezpieczeństwa i sprawozdania oraz materiały robocze z przeprowadzonych sprawdzeń w wybranej gminie. Przeprowadzono wywiady z pracownikami badanej gminy oraz dokonano przeglądu obszarów przetwarzania danych osobowych, np. serwerowni, pomieszczeń monitoringu, archiwum, pomieszczeń biurowych oraz stosowanych systemów informatycznych. Przeprowadzono również badania ankietowe. Wydatki wyszacowano metodą budżetowania „od zera".

Uwarunkowania organizacyjne, techniczne i finansowe wdrożenia RODO

Badana jednostka samorządu terytorialnego jest gminą wiejsko-miejską średniej wielkości. Zajmuje terytorium o powierzchni 200 km^2. Wspólnotę samorządową tworzą mieszkańcy w liczbie około 24 tys. osób. W skład badanej gminy wchodzi ponad 40 sołectw. Zadania wybranej gminy realizują, poza urzędem miasta, jednostki organizacyjne gminy i spółki komunalne. Jednostki gminne realizują zadania z zakresu: pomocy społecznej, gospodarki mieszkaniami komunalnymi, kultury i sportu, opieki zdrowotnej, usług komunalnych takich jak: zaopatrzenie mieszkańców w wodę, odbiór odpadów. Gminie podlega też siedem szkół podstawowych i dwa przedszkola.

Urząd miasta jest zlokalizowany w dwóch budynkach, ale tylko w jednym są przetwarzane dane osobowe. W drugim zlokalizowano salę ślubów, a wolne powierzchnie są udostępniane innym podmiotom.

Budynek, w którym mieści się urząd miasta, jest dwupiętrowy podpiwniczony, łączna powierzchnia zabudowy budynku wynosi 861 m^2, przeciętnie na poziomie jest wyodrębnionych 30 pomieszczeń. W budynku poza urzędem miejskim swoją siedzibę mają trzy jednostki organizacyjne gminy. Kilka pomieszczeń, na różnych poziomach jest wynajmowanych podmiotom trzecim. Opisany budynek stanowi obszar przetwarzania danych osobowych, na który składają się pomieszczenia, gdzie następuje bieżące przetwarzanie danych w ramach obsługi klientów i wykonywania innych prac urzędowych oraz pomieszczenia, gdzie następuje szczególne nagromadzenie danych osobowych, tj. serwerownie i archiwum. Podstawowy budynek urzędu i dane osobowe w nim przetwarzane są zabezpieczone systemem drzwi rozsuwanych z elektroniczną blokadą i kamerami monitoringu miejskiego odsługiwanego przez Straż gminną z siedzibą w budynku urzędu. Klucze do drzwi wejściowych do budynku mają tylko wybrani pracownicy. Drzwi do pomieszczeń biurowych są zamykane na klucz mechaniczny. Pomieszczenia głównej serwerowni i monitoringu miejskiego są zabezpieczone drzwiami antywłamaniowymi klasy C z atestem i elektronicznym systemem kontroli dostępu, okna są oklejone folią antywłamaniową, serwery mają zasilanie awaryjne. Pomieszczenia Wydziału Spraw Obywatelskich są zabezpieczone systemem alarmowym monitorowanym przez firmę Societas i folią antywłamaniową w oknach. Pomieszczenia Straży Miejskiej są zabezpieczone drzwiami antywłamaniowymi klasy C i folią antywłamaniową w oknach. Pomieszczenia archiwum są zabezpieczone drzwiami wzmocnionymi z podwójnym zamkiem mechanicznym, dostęp do okien jest zabezpieczony kratami.

Klucze zapasowe do budynku i pomieszczeń są przechowywane w sejfie. Budynek i pomieszczenia są zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osobom

nieupoważnionym. Pracownicy mogą przebywać w budynku poza godzinami pracy za zgodą burmistrza. Pomieszczenia są sprzątane od godziny 13.00. Sprzątanie w pomieszczeniach podwyższonego nadzoru odbywa się w obecności pracownika odpowiedzialnego za ochronę danych osobowych, w pozostałych pomieszczeniach po godzinach pracy.

W badanej gminie ADO wyznaczył Administratora Bezpieczeństwa Informacji (ABI), a co za tym idzie – określił zakres obowiązków, jakie musi realizować gmina w zakresie ochrony danych osobowych (zob. art. 36a ust. 2 ustawy o ochronie danych osobowych z 1997 roku[3], dalej: u.o.d.o.). Urząd jest w trakcie modyfikacji Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym. Wynikiem przeprowadzonych sprawdzeń jest również:

- wyodrębnienie ponad 50 nowych zbiorów danych osobowych w rozumieniu art. 7 pkt 1 u.o.d.o. i zlikwidowanie 16, w tym zbiorów obejmujących dane wrażliwe;
- założenie Rejestru danych osobowych (obowiązek prowadzenia takiego Rejestru wynika z art. 36a ust. 2 pkt 2 u.o.d.o.);
- uporządkowanie i uzupełnienie Rejestru jawnego;
- wydanie upoważnień do przetwarzania danych osobowych w nowej wersji (rozbudowanej do wszystkich wymaganych prawem elementów), w tym osobom fizycznym współpracującym z gminą na podstawie zróżnicowanych umów zgodnie z art. 37 u.o.d.o. i wprowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych zgodnie z art. 39 ust. 1 u.o.d.o.;
- zawarcie z dostawcami systemów informatycznych i innymi podmiotami świadczącymi usługi, np. kancelarią prawną, umów powierzenia danych osobowych zgodnie z art. 31 u.o.d.o.;
- ograniczenie dostępu do przetwarzania danych w poszczególnych zbiorach do zakresu obowiązków określonych w umowach o pracę, umowach zleceniach itp.;
- dostosowanie uprawnień w systemach informatycznych do faktycznych potrzeb i do rodzaju wykonywanych czynności w zakresie przetwarzania danych osobowych (szczegółowo określonych w art. 7 pkt 2 u.o.d.o.);
- zgłoszenie ujawnionych, wrażliwych zbiorów danych osobowych do Generalnego Inspektora Ochrony Danych Osobowych zgodnie z art. 40 u.o.d.o.

Badana gmina przetwarza wszystkie wyodrębnione zbiory danych osobowych w sposób tradycyjny (w postaci papierowej). Obieg dokumentacji urzędowej, w tym

[3] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922 ze zm.).

korespondencja z klientami, jest wspomagany elektronicznym systemem zarządzania dokumentacją. Rachunkowość gminy jest prowadzona w wielomodułowym systemie SIDAS. Informacje kadrowo-płacowe są przetwarzane w systemie R2płatnik Pro i Płatnik ZUS, a informacje o wykroczeniach, interwencjach i mandatach – w programie e-Mandat. Pełny wykaz eksploatowanych w urzędzie systemów i programów informatycznych wraz z obsługiwanymi zbiorami danych podano w tabeli 1.

Tabela 1. Zestawienie systemów informatycznych, w których przetwarzane są wyodrębniane w urzędzie miasta zbiory danych osobowych

System informatyczny	Zbiór danych osobowych przetwarzany w systemie
program e-Mandat	Rejestr interwencji Ewidencja interwencji z fotoradaru Rejestr bloczków mandatowych Rejestr spraw o wykroczenie Notatki i notatniki służbowe
Technika IT SA z Gliwic	Akta Stanu Cywilnego
SIGID	Użytkownicy wieczyści nieruchomości gminnych Zezwolenia na sprzedaż napojów alkoholowych Zezwolenie na zajęcie pasa drogowego Dzierżawcy, najemcy, użytkownicy majątku gminnego Podatki i opłaty lokalne Sprzedaż nieruchomości Opłaty za gospodarowanie odpadami komunalnymi Dochody z majątku gminnego Kontrahenci Sołtysi Gminy Trzebnica Wpłaty i wypłaty Dłużnicy
EZD	Korespondencja – Biuro Obsługi Klienta Wpłaty i wypłaty Dłużnicy
Program do obsługi Lokalnego Rejestru Mieszkańców i Rejestru Wyborców	Ewidencja ludności
System monitoringu wizyjnego	Monitoring miejski
R2płatnik Pro i Płatnik ZUS	Radni miasta i gminy Pracownicy zatrudnieni na podstawie umowy o pracę Pracownicy zatrudnieni na podstawie umów cywilno-prawnych Rekompensaty za ćwiczenia wojskowe

Źródło: opracowanie własne.

Dostęp do wyżej wymienionych systemów jest możliwy z komputerów połączonych z siecią publiczną, co zgodnie z § 6 ust. 4 Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[4] (RBSI), oznacza konieczność stosowania środków bezpieczeństwa systemów informatycznych na wysokim poziomie (zob. część C załącznika do wyżej wskazanego rozporządzenia).

Analizę zabezpieczenia systemów informatycznych eksploatowanych w urzędzie przeprowadzono za pomocą kwestionariusza. Wyniki badania wskazują, że eksploatowane systemy nie pozwalają automatycznie rejestrować: użytkownika, dat wprowadzenia danych, odbiorców informacji oraz sprzeciwu osoby, której dane są przetwarzane. Hasła służące do uwierzytelnienia użytkownika są łatwe do złamania i nie są systematycznie zmieniane. We wskazanym zakresie systemy nie spełniają więc wymagań RBSI.

W części jednostek podległych gminie, tj. szkoły, przedszkola, spółki komunalne, opracowano i wdrożono polityki bezpieczeństwa informacji z instrukcjami zarządzania systemami informatycznymi.

Z punktu widzenia kondycji finansowej warunkującej możliwości dostosowania zabezpieczeń danych osobowych do zwiększonych wymagań badana gmina ma dobrą sytuację. We wszystkich latach przyjętych do analizy gmina spełnia relacje określające dopuszczalny poziom zadłużenia gminy ujęte w art. 243 ustawy o finansach publicznych[5]. Corocznie znacząco przyrasta budżet gminy, w 2016 dochody gminy wzrosły o 29%, a dochody własne o 20%. Gmina realizuje w każdym roku budżetowym ponad 100 inwestycji, w tym kilka dużych, takich jak budowa hali sportowej, przebudowa basenu, przychodni zdrowia, centrum kultury. Ze względu na realizowane inwestycje zauważalne jest przesuwanie środków między poszczególnymi budżetami. W dłuższym okresie niedobory i nadwyżki bilansują się.

Uwzględniając powyższe, można stwierdzić, że dane osobowe przetwarzane w badanej gminie nie są w pełni chronione tak, jak przewidziano w obowiązującym do 25 maja 2018 roku prawodawstwie. Mimo to w gminie nigdy nie miały miejsca znaczące naruszenia danych osobowych. Bardzo istotnym czynnikiem zdecydowanie zwiększającym bezpieczeństwo przetwarzania informacji, w tym danych osobowych w gminie, jest kultura organizacyjna urzędu. Systemy wartości przestrzegane przez pracowników

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

[5] Ustawa z dnia z dnia 27 sierpnia 2009 r. o finansach publicznych (t. j. Dz. U. z 2017 r. poz. 2077 ze zm.).

urzędu i jego kierownictwo, właściwy klimat oraz system wzorów myślenia i działania utrwalone w środowisku społecznym gminy ułatwiają realizację wszystkich celów gminy, w tym bezpiecznego przetwarzania danych osobowych.

Identyfikacja obszarów i wydatków oraz pomiar kosztów i nakładów

Celem RODO jest ujednolicenie standardów przetwarzania danych osobowych we wszystkich państwach członkowskich UE. Wprowadzone wymagania stanowią zdecydowanie większe wyzwanie dla ADO niż dotychczas obowiązujące regulacje krajowe, choć są obszary RODO, w których zapisy są analogiczne z u.o.d.o. Są też regulacje u.o.d.o., których nie przewiduje RODO, np. rejestracja zbiorów danych osobowych, ale są też regulacje wprowadzone przez RODO i to głównie ich przyjęcie będzie wymagało dodatkowego zaangażowania potencjału ADO. Do nowych obszarów istotnych dla gminy można zaliczyć:

1. Obowiązek udowodnienia przez ADO, że stosuje odpowiednią ochronę przetwarzanych danych osobowych. W spełnianiu tego obowiązku ma pomóc stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO, lub zatwierdzony mechanizmu certyfikacji, o którym mowa w art. 42 RODO. Certyfikacja jest dobrowolna.
2. Nowe prawa obywateli, tj. „prawo do bycia zapomnianym" (art. 17 RODO), czyli prawo życzenia sobie, aby dane zostały usunięte, również w systemach informatycznych, prawo do ograniczenia przetwarzania danych (art. 18 RODO; w takiej sytuacji ADO nie może przechowywać danych), uprawnienie do żądania przenoszenia danych (art. 20 RODO), jeśli są one przetwarzane w systemach informatycznych. ADO, do którego osoba chce przenieść informacje, nie jest jednak zobowiązany do ich przyjęcia.
3. Obowiązek Administratora o powiadomieniu wszystkich odbiorców danych o sprostowaniu danych, ograniczeniu przetwarzania i usunięciu danych (art. 19 RODO).
4. Obowiązek przeprowadzania bieżącej oceny skutków dla ochrony danych (art. 24 i motyw 83 RODO). W tym zakresie ADO może się posiłkować normą 31000:2009[6] i/lub kodeksem postepowania, jeśli taki przygotują i opublikują podmioty wskazane w art. 40 RODO. Na chwilę obecną takich kodeksów nie opublikowano.

[6] Na normę ISO 31000:2009 składają się: ISO Guide 73:2009 – Zarządzanie ryzykiem – Słownictwo – wytyczne dla standardów (Risk management – Vocabulary – Guidelines for use in standards), ISO 31000:2009 – Zarządzanie ryzykiem – zasady i wytyczne (Risk management – Principles and guidelines), ISO/IEC 31010:2009 – Zarządzanie ryzykiem – Metody szacowania ryzyka (Risk management – Risk assessment techniques), https://wiedza.pkn.pl/web/wiedza-normalizacyjna/zarzadzanie-ryzykiem [dostęp: 05.06.2018].

Ocena skutków dla ochrony danych osobowych będzie niczym innym, jak oceną systemu zarządzania ryzykiem i będzie wymagała: 1) zdefiniowania i określenia każdego ryzyka zagrażającego ADO wraz z określeniem źródeł ryzyka, przyczyn i możliwych szkód im towarzyszących, 2) oszacowania prawdopodobieństwa wystąpienia zdefiniowanych rodzajów ryzyka oraz wartości prawdopodobnych strat, 3) redukcji ryzyka przekraczającego akceptowalny próg (możliwe działania: uniknięcie ryzyka poprzez wycofanie się lub zaprzestanie działań wywołujących ryzyko, zmniejszenie prawdopodobieństwa wystąpienia ryzyka przez zastosowanie dodatkowych środków zabezpieczających, zmianę następstw, podzielenie się ryzykiem z inną osobą albo świadome utrzymanie ryzyka), 4) komunikowania ryzyka zarówno między uczestnikami procesu przetwarzania danych, jak i z decydentami w podmiocie oraz z ADO i IOD, i ewentualnie z organem nadzorczym w zakresie ochrony danych osobowych[7]. ADO nie ma obowiązku wykonania oceny w sytuacji, gdy przetwarzanie następuje na podstawie obowiązku prawnego lub ze względu na istniejący interes publiczny, a są to dominujące podstawy przetwarzania danych osobowych w gminie. W RODO założono jednak, że we wskazanym zakresie w prawie UE lub prawie państwa członkowskiego uregulowano daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji przed przyjęciem tej podstawy prawnej. Obowiązujące na dzień dzisiejszy regulacje krajowe nie były sprawdzane pod względem spełnienia tego wymogu. Należy oczekiwać wyjaśnienia organu nadzorczego w tym zakresie, może w ramach tworzenia wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (zob. art. 34 ust. 4 RODO). Ocena skutków ma mieć charakter obiektywny (motyw 76 RODO) i ma jej dokonać ADO, co w praktyce będzie oznaczało konieczność skorzystania z usługi wyspecjalizowanego podmiotu.

5. Obowiązek wdrożenia i uaktualniania odpowiednich środków organizacyjnych i technicznych adekwatnych do ryzyka: przypadkowego lub niezgodnego z prawem zniszczenia danych, utraty, modyfikacji, nieuprawnionego ujawnienia i dostępu do danych (art. 24 ust. 1 RODO). Podstawą określenia środków zabezpieczających musi być analiza ryzyka systemu ochrony danych osobowych (art. 32 RODO), której zasadniczą częścią też będzie ocena systemu zarządzania ryzykiem, podobnie jak w ocenie skutków dla danych osobowych. Ocena, czy ADO zastosował „odpowiednie środki", będzie bardzo dyskusyjna, zwłaszcza w sytuacji naruszenia

[7] Jeżeli ocena skutków dla ochrony danych wykaże wysokie ryzyko, a ADO nie jest w stanie go zminimalizować, uwzględniając dostępną technologię i rozsądne koszty wdrożenia zabezpieczeń, to przed rozpoczęciem czynności przetwarzania należy skonsultować się z organem nadzorczym.

danych osobowych. Stąd też wydaje się zasadnym zlecanie podmiotom zewnętrznym niezależnych, obiektywnych opinii. W ustawie wskazano bezpośrednio cztery sposoby bezpiecznego przetwarzania danych osobowych, a mianowicie (art. 32 ust. 1 RODO): pseudonimizację i szyfrowanie danych osobowych; zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Skuteczność zabezpieczeń systemów informatycznych można badać np. za pomocą testów penetracyjnych[8].

6. Koncepcję *privacy by design* i *privacy by default* (art. 25 RODO), która nakłada na ADO obowiązek uwzględniania ochrony danych osobowych w fazie projektowania oraz ustawienia domyślnej ochrony danych osobowych w produktach i usługach. To oznacza, że w systemach informatycznych oferowanych przez dostawców ochrona danych osobowych ma być aktywowana domyślnie. Podkreśla się, iż obowiązkiem ADO jest wdrożenie takich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były jedynie te dane, które są niezbędne dla osiągnięcia danego celu przetwarzania, czyli że należy przetwarzać jak najmniejszą liczbę danych, ograniczyć do minimum zakres przetwarzania, okres przetwarzania i dostępność do danych. Mechanizmy te mają zapewnić maksymalną ochronę użytkownika również w przetargach publicznych. ADO w tym zakresie może stosować takie mechanizmy jak szybka pseudonimizacja czy inwentaryzacja dokumentacji archiwalnej.
7. Prowadzenie Rejestru czynności przetwarzania (art. 30 RODO), który powinien zawierać informacje o: ADO (nazwa, dane kontaktowe), celu przetwarzania, kategorii osób, których dane dotyczą, kategorii danych osobowych, kategorii odbiorców danych, państwach trzecich lub instytucjach międzynarodowych, do których przekazywane są dane, planowanym terminie usunięcia poszczególnych kategorii danych, sposobach technicznych i organizacyjnych zabezpieczenia. Podany zakres w praktyce nieznacznie będzie się różnił od aktualnie prowadzonych Rejestrów zbiorów danych osobowych. O udostępnienie Rejestru czynności może wystąpić organ nadzorczy.
8. Zgłaszanie do organu nadzorczego naruszeń (incydentów fizycznych i technicznych; art. 33 RODO) za pomocą systemu informatycznego udostępnionego przez organ

[8] A. Dmochowska, M. Zadrożny, *Unijna reforma ochrony danych osobowych – analiza zmian*, C.H. Beck, Warszawa 2016.

nadzorczy i informowanie osoby, której dane zostały ujawnione (art. 34 RODO), w przypadku, gdy ujawnienie może skutkować zagrożeniem praw i swobód osób. ADO może nie zgłaszać naruszeń, jeśli udowodni, że jest mało prawdopodobne, by naruszenie skutkowało powstaniem uszczerbku fizycznego, utratą kontroli nad własnymi danymi osobowymi, ograniczeniem praw, dyskryminacją, kradzieżą lub sfałszowaniem tożsamości, stratą finansową, nieuprawnionym odwróceniem pseudonimizacji, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową[9]. Można przypuszczać, że ciążący na ADO obowiązek udowodnienia małego ryzyka wystąpienia negatywnych skutków naruszenia danych osobowych spowoduje, że dla uniknięcia kary ADO będzie zgłaszał większość incydentów. ADO ma również obowiązek dokumentować naruszenia wraz z okolicznościami ich wystąpienia, skutkami i podjętymi działaniami zaradczymi. Przyjęta dokumentacja musi przekonać organ nadzorczy, że ADO odpowiednio do ryzyka naruszania chroni dane osobowe, czyli stosuje wystarczające polityki, środki ochrony technicznej i organizacyjnej.

9. Obowiązek wyznaczenia w instytucjach publicznych Inspektorów Ochrony Danych Osobowych (IOD), który dysponuje wiedzą ekspercką z zakresu danych osobowych. Art. 37 ust. 3 zezwala na powołanie jednego inspektora ochrony danych osobowych dla kilku podmiotów, organów publicznych. IOD musi być związany umową z ADO. Obowiązkiem ADO jest też dokształcanie powołanego inspektora.

Zapisy RODO wymuszają również zmiany w zakresie:

1) prawa dostępu i wglądu obywatela w jego dane. ADO został zobowiązany do podjęcia środków, które pozwolą mu w sposób zrozumiały i łatwo przyswajalny komunikować się z osobą (zob. art. 12 RODO), której dane przetwarza, co oznacza konieczność stosowania wielu wzorów dokumentów dostosowanych do np. grup wiekowych osób. ADO może udzielać informacji pisemnie i drogą elektroniczną, generalnie w taki sposób, w jaki osoba fizyczna złożyła żądanie. Wszelkie informacje mają być udzielane niezwłocznie (do miesiąca, a w szczególnie trudnych przypadkach do 3 miesięcy). Zgodnie z art. 15 ust. 3 RODO ADO ma obowiązek dostarczyć osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu, czyli kopie dokumentów, w których widoczne są dane osobowe. Za podjęte działania ADO nie może pobierać opłat, chyba że żądania osoby są nadmierne lub nieuzasadnione. W ostatnim przypadku ADO może nie udzielić informacji, ale na nim spoczywa udowodnienie, że żądania osoby są nadmierne

[9] W treści 75 motywu preambuły RODO wyszczególniono zagrożenia związane z przetwarzaniem danych, ze wskazaniem zagrożeń prowadzących do uszczerbku fizycznego albo szkód majątkowych lub niemajątkowych.

lub nieuzasadnione. Taki zapis różni się zdecydowanie od obowiązującej obecnie normy zawartej w art. 32 ust. 5 UODO, ograniczającej możliwość skorzystania z prawa do informacji, nie częściej niż raz na 6 miesięcy. ADO ma obowiązek jednoznacznego zidentyfikowania tożsamości osoby przed udzieleniem informacji przez zebranie dodatkowych informacji;

2) obowiązku informacyjnego. Zbierając dane od osoby, ADO ma obowiązek przekazania informacji rozszerzonej w stosunku do aktualnie wymaganej w u.o.d.o. (art. 13 i 14 RODO):
   a) dane kontaktowe IOD,
   b) podstawę prawną przetwarzania,
   c) informacje o odbiorcach danych lub kategoriach odbiorców,
   d) informacje o zamiarze przekazania danych do państwa trzeciego, czyli poza UE,
   e) okres, przez który dane będą przetwarzane lub kryteria ustalenia tego okresu,
   f) informacje o prawie żądania spełnienia praw przysługujących osobie fizycznej, w tym o nowych prawach: cofnięcia zgody, „prawie do bycia zapomnianym";
   g) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym albo warunkiem zawarcia umowy oraz czy dana osoba jest zobowiązana do ich podania i o przewidywanych konsekwencjach niepodania danych;
   h) źródle pochodzenia danych, jeśli pozyskano dane w inny sposób niż od osoby, której dane dotyczą.

   Obowiązek informowania osoby nie jest wymagany, jeśli w przepisach prawa krajowego lub UE wyraźnie uregulowano pozyskiwanie lub ujawnianie danych osobowych (art. 14 ust. 5 pkt c RODO). Jest to istotna zmiana w stosunku do stanu aktualnego, która znacząco zwiększy w badanej gminie krąg osób, wobec których będzie musiała zrealizować obowiązek informacyjny. Do tej pory wyłączenie z obowiązku informacyjnego następowało już w sytuacji wskazania podstawy prawnej do przetwarzania danych, czyli np. Ustawy o dostępie do informacji publicznej, a nie konkretnego artykułu tej ustawy, w którym zostały wymienione dane osobowe pozyskiwane od osoby składającej wniosek o udostępnienie danych[10].

3) upoważnienia do przetwarzania danych osobowych, które będą nadal wymagane (art. 32 ust. 4 RODO). W przepisach nie określono ani formy, ani zakresu informacji, które powinny być w nim ujęte. Upoważnienie jest jednym z elementów zabezpieczeń organizacyjnych. Poprzez przyjętą więc konstrukcję upoważnienia

[10] A. Balicki (red.), *Ochrona danych osobowych w sektorze publicznym z uwzględnieniem ogólnego rozporządzenia unijnego*, C.H. Beck, Warszawa 2016, s. 193-195.

ADO będzie realizował swój podstawowy obowiązek: dobrania rozwiązań technicznych i organizacyjnych adekwatnych do ryzyk naruszenia danych. Wydaje się, że w świetle dotychczasowych wyjaśnień do RODO stosowany w badanej gminie wzór upoważnienia jest wystarczający;

4) powierzenia przetwarzania danych. Jeśli gmina przetwarza dane we wspólnym celu z innym podmiotem (takie warunki są spełnione w wielu przypadkach między podmiotami publicznymi), będzie mogła zastąpić umowy/porozumienia z innymi podmiotami umowami o współadministrowaniu zgodnie z art. 26 RODO. W pozostałych przypadkach nadal konieczna jest pisemna umowa powierzenia. W art. 28 ust. 3 RODO podano szczególne elementy takiej umowy zapisując, że podmiot przetwarzający musi zobowiązać się do: zachowania danych w tajemnicy, do podjęcia wszelkich środków bezpieczeństwa przetwarzania wymaganych art. 32 RODO, przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego, usunięcia lub zwrócenia wszelkich danych, usunięcia kopii z chwilą zakończenia przetwarzania, umożliwienia ADO przeprowadzania audytów i kontroli, a także pomocy ADO w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, wywiązywania się z obowiązków dotyczących bezpiecznego przetwarzania, zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu, zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, oceny skutków dla ochrony danych i uprzednich konsultacji z GIODO. Analiza porównawcza stosowanego w badanej gminie wzoru umowy powierzenia i wymienionych elementów umowy w art. 28 ust. 3 RODO wskazuje, że stosowaną umowę należy uzupełnić o zobowiązanie podmiotu przetwarzającego do pomocy w zakresach wymienionych wyżej.

Uwzględniając wskazane powyżej nowe obszary regulacji problematyki ochrony danych osobowych i zmiany w stosowanych przepisach, dokonano identyfikacji kosztów i nakładów, które powinny być poniesione, aby badana gmina spełniała nowe wymagania prawne. Do kosztów zaliczono przewidywane, celowe i ekwiwalentne zużycie czynników działalności[11] o charakterze bezpośrednim dla wskazanych działań, czyli takie, które można jednoznacznie przyporządkować do działania. Pojęcie nakładów przyjęto w węższym zakresie jako wydatki na pozyskanie rzeczowych oraz niematerialnych i prawnych aktywów[12]. Specyfikację kosztów bezpośrednich niezbędnych działań dostosowawczych podano w tabeli 2. Jak można zauważyć, badana gmina będzie musiała zakupić przynajmniej trzy licencje na specjalistyczne oprogramowanie i ponieść głównie

[11] Przyjęto definicję za: D. Sołtys (red.), *Rachunkowość zarządcza. Rachunek kosztów*, Wydawnictwo UE we Wrocławiu, Wrocław 2014, s. 21.

[12] Por. art. 28 ustawy z dnia 29 września 1994 r. o rachunkowości (t. j. Dz. U. z 2018 r. poz. 395 ze zm.).

koszty specjalistycznych usług obcych, w tym wykonania analiz ryzyka i testów bezpieczeństwa oraz szkoleń zewnętrznych w zakresie, w którym IOD nie będzie miał wystarczających kwalifikacji. Ewentualne kary administracyjne i odszkodowania oraz zadośćuczynienia zasądzone w postępowaniach cywilnych będą stanowiły koszty pozostałej działalności operacyjnej. Według klasyfikacji budżetowej wszystkie wskazane koszty i nakłady będą stanowiły wydatki bieżące.

Tabela 2. Obszary zmian oraz rodzaje wydatków niezbędnych do wdrożenia RODO w badanej gminie

Lp.	Zakres zmian	Działanie	Bezpośrednie koszty wg rodzajów działalności/rodzaju kosztów lub/i nakłady
1	Obowiązek informacyjny	1. przesłanie/przekazania osobiste informacji z kopiami dokumentów, 2. szkolenie pracowników	Koszty: wynagrodzenia z pochodnymi, zużycie materiałów biurowych
2	Prawa osób, których dane są przetwarzane (do sprostowania, przeniesienia danych, ograniczenia przetwarzania, sprzeciwu)	1. wykonanie woli osób, 2. inwentaryzacja i usunięcie dokumentacji papierowej lub anonimizacja, 3. usunięcie rekordów w systemach informatycznych lub zablokowanie danych, 4. przekazanie informacji odbiorcom o zrealizowanej woli osób fizycznych, 5. dostosowanie systemów informatycznych do przekazywania danych osobom fizycznym w powszechnie używanym formacie nadającym się do odczytu maszynowego, 6. Wewnętrzne szkolenie pracowników	Koszty: wynagrodzenia z pochodnymi, usługa niszczenia dokumentacji przez podmiot spełniający wymagania RODO w zakresie ochrony danych osobowych, zużycie materiałów biurowych amortyzacja licencji Nakłady: zakup licencji na oprogramowanie
3	Bieżąca ocena skutków dla ochrony danych i uzgodnienia z organem nadzorczym/analiza ryzyka dla doboru odpowiednich środków bezpieczeństwa	1. zlecenie usługi, 2. szkolenie IOD	Koszty: usługi obce
4	Uaktualnienie stosowanych zabezpieczeń organizacyjnych (polityki bezpieczeństwa, rejestru zbiorów danych osobowych, upoważnień, umów powierzenia)	1. aktualizacja polityki bezpieczeństwa, rejestru zbiorów danych osobowych, upoważnień, umów powierzenia, 2. wewnętrzne szkolenie pracowników	Koszty: wynagrodzenia z pochodnymi

Lp.	Zakres zmian	Działanie	Bezpośrednie koszty wg rodzajów działalności/rodzaju kosztów lub/i nakłady
5	Koncepcja *privacy by design* i *privacy by default*	1. ujęcie zasad w polityce bezpieczeństwa, wprowadzenie zmian zarządzeniem Burmistrza, 2. wewnętrzne szkolenie kadry kierowniczej	Koszty: wynagrodzenia z pochodnymi
6	Zgłaszanie i dokumentowanie naruszeń	1. opracowanie wzoru zgłoszenia, 2. zbieranie dokumentacji potwierdzającej naruszenie i ocena skutków, 3. sporządzanie zgłoszeń i prowadzenie rejestru naruszeń	Koszty: wynagrodzenia z pochodnymi
7	Zatrudnienie IOD	1. powierzenie obowiązków dotychczasowemu ABI, 2. szkolenia zewnętrzne	Koszty: wynagrodzenia, zużycie materiałów biurowych, ubezpieczenia społeczne i inne świadczenia dla pracowników, amortyzacja licencji Nakłady: zakup licencji programu do zarządzania ochroną danych osobowych (zarządzania upoważnieniami, prowadzenia rejestru czynności, rejestru naruszeń)
8	Wdrożenie zabezpieczeń systemów informatycznych	1. zakup licencji na program do szyfrowania danych, 2. zlecenie przeprowadzania testów	Koszty: amortyzacja licencji usługi obce Nakłady: zakup licencji na oprogramowanie
9	Testowanie pracowników metodami socjotechnicznymi	1. zlecenie przeprowadzania testów, 2. szklenia zewnętrzne z zakresu cyberprzestępczości, w tym ataków socjotechnicznych	Koszty: usługi obce
10	Odpowiedzialność za nieuzasadnione udostępnienie informacji		Koszty: pozostałe koszty operacyjne
11	Odszkodowanie za przetwarzanie danych w sposób niezgodny z RODO		Koszty: pozostałe koszty operacyjne

Źródło: opracowanie własne.

W tabeli nr 3 ujęto wstępne szacunki rocznych kosztów i nakładów na wdrożenie i stosowanie RODO w badanej gminie. Podane kwoty oszacowano metodą budżetowania „od zera"[13], głównie na podstawie pozyskanych ofert. Szczególną uwagę należy zwrócić na pozycję „Zakup licencji – realizacja uprawnień obywateli". W prezentowanym zestawieniu przyjęto, iż dostawcy oprogramowania już eksploatowanego w gminie zaproponują do swoich systemów dodatkowe funkcje pozwalające automatycznie rejestrować np. datę wprowadzenia danych do systemu, osobę wprowadzającą, wykonanie dyspozycji osoby fizycznej, np. sprzeciwu, czy operacje na danych, np. przekazania do przetwarzania innemu podmiotowi, a także sporządzać raporty/sprawozdania z przetwarzania danych osobowych. W przeciwnym wypadku gmina musiałaby wymienić wszystkie eksploatowane systemy informatyczne na nowe, posiadające funkcjonalności wymagane RODO. Czy wydatek rzędu kilku milionów można by uznać za rozsądny, zgodnie z motywem 94 RODO, w porównaniu z ryzykiem naruszenia danych osobowych? Odpowiedzi na to dyskusyjne pytanie należy oczekiwać w zatwierdzonych kodeksach postępowania dla administracji publicznej.

Wydatki na wdrożenie RODO w badanej gminie wyszacowano na poziom około 99 tys. zł, co stanowi ułamkową część budżetu gminy.

Tabela 3. Obszary zmian oraz rodzaje wydatków niezbędnych do wdrożenia i stosowania RODO w badanej gminie

Lp.	Pozycja kosztów lub nakładów	Ilość	Stawka jednostkowa	Szacunkowy wydatek roczny (w zł)
1	Zatrudnienie IOD w jednostkach gminy	14	500	7 000,00
2	Zużycie materiałów biurowych			3 929,00
3	Szkolenia zewnętrzne dla IOD i z zakresu cyberprzestępczości i technik socjotechnicznych dla pracowników urzędu	1	5 000,00	5 000,00
4	Analiza skutków/analiza ryzyka	1	12 300,00	12 300,00
5	Niszczenie dokumentów	2	615,00	1 230,00
6	Zakup licencji – program wspomagający ABI	1	1 845,00	1 845,00
7	Zakup licencji – realizacja uprawnień obywateli	110	369,00	40 590,00
8	Zakup licencji – szyfrowanie danych wysyłanych i dysków w komputerach	110	246,00	27 060,00
	Razem			98 954,00

Źródło: opracowanie własne.

[13] Metodę budżetowania „od zera" stosuje się wówczas, gdy procesy są realizowane w jednostce po raz pierwszy.

Należy dodać, że poza kosztami bezpośrednimi gmina będzie ponosiła koszty niezwiązane wprost ze wskazanymi działaniami (koszty pośrednie). Przez zwiększenie zakresu obowiązków pracowników gminy, np. w celu spełnienia obowiązku informacyjnego, dokumentowania tego obowiązku, część kosztów pracy pracowników i kosztów funkcjonowania pracowników w obiekcie gminnym będzie stanowiła koszty pośrednie stosowania RODO. W identyfikacji niezbędnych działań i szacunkach kosztów założono, że zakres podejmowanych zmian dostosowawczych nie może wywołać zatrudnienia dodatkowych pracowników obsługujących interesantów.

Podsumowanie

Celem artykułu było oszacowanie niezbędnych wydatków na wdrożenie nowych wymagań Unii Europejskiej w zakresie ochrony danych osobowych w wybranej gminie. Zakres zadań gmin powoduje, że jednostki te przetwarzają dane osobowe licznych osób, porządkowane według wielu kryteriów i obejmujące również dane podlegające szczególnej ochronie, powszechnie określane jako tzw. wrażliwe. Na około sto wyodrębnionych zbiorów danych osobowych w badanej gminie 25 pozwala bezpośrednio lub pośrednio zidentyfikować osoby na podstawie danych szczególnie chronionych.

Analiza uwarunkowań organizacyjnych i technicznych przetwarzania danych osobowych w badanej gminie pozwala stwierdzić, iż tak jak w wielu podmiotach, w tym publicznych, dane osób fizycznych nie są w pełni chronione, czyli tak jak określono to w obowiązujących poprzednio przepisach. Szczególnie istotne są ograniczenia eksploatowanych systemów, programów komputerowych. Nie rejestrują one informacji o działaniach na danych osobowych, co jest wymagane RBSI od 2004 roku. W badanej gminie nie doszło nigdy do ujawnienia danych osobowych. Bardzo istotnym czynnikiem zdecydowanie zwiększającym bezpieczeństwo przetwarzania informacji, w tym danych osobowych w wybranej gminie jest kultura organizacyjna urzędu. Systemy wartości przestrzegane przez pracowników urzędu i jego kierownictwo, właściwy klimat oraz system wzorów myślenia i działania utrwalone w środowisku społecznym wybranej gminy ułatwiają realizację wszystkich celów gminy, w tym bezpiecznego przetwarzania danych osobowych.

Porównanie zmodyfikowanych zabezpieczeń organizacyjnych danych osobowych w gminie w części, która była dotychczas regulowana, pozwala stwierdzić, że opracowana dokumentacja ochrony danych osobowych będzie wymagała niewielkich zmian. Przyjęte wzory dokumentacji są generalnie zgodne z nowymi wymaganiami. Nadal dyskusyjne pozostaje wykonywanie obowiązku informacyjnego przez podmiot publiczny, który przetwarza dane osobowe głównie na podstawie obowiązujących przepisów,

wykonując swoje zadania i dopełniając obowiązki ciążące na gminie. Zmian będzie wymagał Rejestr zbiorów danych osobowych, który musi zostać przekształcony w Rejestr czynności przetwarzania. Oczywiście konieczne będzie wprowadzenie nowych wymagań, np. prowadzenie Rejestru naruszenia danych osobowych i zgłaszanie incydentów do organu nadzorczego czy zatrudnienie IOD we wszystkich jednostkach publicznych podległych gminie. Największym wyzwaniem będzie dostosowanie funkcjonalności systemów informatycznych do przetwarzania danych osobowych zgodnie z zasadami RODO, czyli w sposób integralny, poufny i rozliczalny (art. 5 RODO). Jeśli dostawcy systemów informatycznych przygotują programy dostosowujące swoje produkty do nowych wymagań, to roczne wydatki na wdrożenie i stosowane wymagań RODO w badanej gminie ukształtują się na poziomie około 99 tys. zł. Oszacowana kwota stanowi ułamkową część budżetu wybranej gminy.

Bibliografia

Akty prawne

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922 ze zm.).

Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t. j. Dz. U 2017 r. poz. 2077 ze zm.).

Ustawa z dnia 29 września 1994 r. o rachunkowości (t. j. Dz. U. z 2018 r. poz. 395 ze zm.).

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

Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016).

Literatura

Balicki A. (red.), *Ochrona danych osobowych w sektorze publicznym z uwzględnieniem ogólnego rozporządzenia unijnego*, C.H. Beck, Warszawa 2016.

Dmochowska A., Zadrożny M., *Unijna reforma ochrony danych osobowych – analiza zmian*, C.H. Beck, Warszawa 2016.

Sołtys D. (red.), *Rachunkowość zarządcza. Rachunek kosztów*, Wydawnictwo UE we Wrocławiu, Wrocław 2014.

Internet

PN-ISO 31000:2009 - wersja polska, https://wiedza.pkn.pl/web/wiedza-normalizacyjna/zarzadzanie-ryzykiem [dostęp: 05.06.2018].

Expenditure on the implementation of new legal regulations in the field of personal data protection on the example of a selected municipality.

Summary

In connection with the obligation of direct application by the member states of the European Union of European Parliament and Council Regulations, entities processing personal data are obliged, from May 2018, to comply with the new standards set in General Data Protection Regulation (EU) 2016/679 from 27th April 2016 on data protection and privacy for all individuals, free flow of such data and on superseding the Data Protection Directive 95/46/EC). In the article the direct costs of necessary adaptation activities were estimated as well as expenditure on infrastructure operated by the studied municipality, mainly IT.

Keywords

personal data protection, GDPR, costs, cost accounting, local government units