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

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2018.131/1-19 | strony: 193–201

Mateusz Kuczabski
Akademia Sztuki Wojennej
Wydział Bezpieczeństwa Narodowego
Instytut Studiów Strategicznych
Katedra Bezpieczeństwa Informacyjnego i Komunikacji
mateusz.kuczabski@piastunzoz.pl

Adaptacja architektury systemów bezpieczeństwa w sektorze ochrony zdrowia do nowych wymagań RODO

Kod JEL: I 11
Słowa kluczowe: bezpieczeństwo, ochrona danych, system informatyczny, zdrowie, GDPR
Streszczenie. Wprowadzenie przez Parlament Europejski nowych przepisów dotyczących ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych, zmusza sektor ochrony zdrowia do podjęcia działań auditowych z następowym wprowadzenia zmian w istniejących systemach informatycznych. Nowe przepisy określają konieczność wbudowania funkcji ochrony prywatności na każdym etapie projektowania systemu, a wysoki poziom bezpieczeństwa musi być narzucony domyślnie dla każego użytkownika. Artykuł poświęcono analizie wprowadzanych rozwiązań, by na tej podstawie sformułować przypuszczalne konsekwencje i realne możliwości adaptacji podmiotów ochrony zdrowia do implementacji wymagań.

Wprowadzenie

Rozwiązania IT, funkcjonujące w podmiotach ochrony zdrowia, stanowią jeden z kluczowych elementów jakości opieki nad pacjentami. Poprawiają komunikację, usprawniają wzajemne relacje między interesariuszami systemu, a jednocześnie mają zapewniać bezpieczeństwo danych wykorzystywanych w systemie. Natomiast samą cyfryzację, tzw. e-zdrowie, można analizować w dwóch wymiarach: na poziomie ogólnopolskiego systemu ochrony zdrowia oraz samych podmiotów – placówek medycznych do niego należących (Kuczabski, 2009). Niestety, istniejące w tym zakresie rozwiązania są niezadowalające i plasują Polskę wśród krajów europejskich, według Europejskiego Konsumenckiego Indeksu Zdrowia 2016, uwzględniającego także i inne ana-

lizowane czynniki, na dalekiej 31. pozycji, tym samym wyprzedzając jedynie Rumunię, Czarnogórę, Bułgarię i Albanię. Do lidera, którym jest Holandia, brakuje 363 punktów (EHCI, 2017). Autor opracowania, oceniając cyfryzację, uwzględnił m.in. takie wskaźniki, jak internetowe lub dostępne telefonicznie całą dobę interaktywne źródła informacji o systemie opieki zdrowotnej (1.7), dostęp pacjentów do internetowych systemów umawiania wizyt (1.11), e-recepty (1.12), ale – co szczególnie istotne w kontekście bezpieczeństwa informacji – rozpowszechnianie elektronicznej dokumentacji medycznej (1.10).

Jak z tego wynika, aktualnie na obu wymienionych wcześniej poziomach, sektor ochrony zdrowia nie dysponuje jednolitym i kompleksowym rozwiązaniem, które pozwoliłoby sprostać wszystkim wprowadzanym wymaganiom określonym w rozporządzeniu unijnym dotyczącym ochrony danych osobowych (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), które zacznie obowiązywać w połowie 2018 roku. Wydaje się więc celowym poddać ocenie i wskazać najważniejsze elementy, które wpływają na brak optymalnych rozwiązań adaptacyjnych sektora ochrony zdrowia. Po pierwsze, przyczyny tego stanu należy dopatrywać w fakcie, że dotychczas na gruncie prawa europejskiego nie istniały zasady odnoszące się do prywatności i bezpieczeństwa danych, które byłyby tak silnie osadzone w koncepcji modelu cyklu życia systemu informatycznego. Po drugie, wynika to także ze zróżnicowania poszczególnych sposobów przechowywania dokumentacji medycznej, jakie funkcjonują w podmiotach sektora ochrony zdrowia. Zróżnicowanie to powoduje rozdrobnienie odpowiedzialności za system ochrony i bezpieczeństwa przetwarzanych danych.

Model cyklu życia systemu informatycznego (oprogramowania) to szereg wzajemnie zależnych od siebie etapów, czynności rozłożonych w czasie odbywających się podczas pracy nad opracowaniem i wyprodukowaniem systemu określonego typu oraz jego eksploatacji. Cykl ten obejmuje okres od powstania u użytkownika potrzeby budowy systemu informatycznego, przez prezentację jego idei, konstrukcję, użytkowanie, przystosowanie do ewentualnych zmian funkcjonowania, na wycofaniu z eksploatacji kończąc (Makuchowski, 2016).

Obserwowane w sektorze ochrony zdrowia zróżnicowanie sposobów przechowywania dokumentacji medycznej wpływa bezpośrednio na podział kontroli i odpowiedzialności pomiędzy usługodawcą a podmiotem zewnętrznym. Obecnie w znacznym stopniu utrudnia to administratorowi danych zagwarantowanie bezpieczeństwa danych osobowych, a zmiana przepisów dotyczących ochrony danych osobowych wprowadzona GDPR, właśnie na administratorów danych nakłada szereg nowych obowiązków.

1. Ochrona danych osobowych

Przetwarzanie informacji przez podmioty sektora ochrony zdrowia jest ściśle związane z istniejącymi możliwościami dostępu pacjentów do własnej dokumentacji medycznej. Mimo jasnych w tym zakresie zapisów wynikających z dyrektywy UE o ochronie danych osobowych, która stanowi jednoznacznie, że pacjentowi takie uprawnienie powinno przysługiwać z mocy prawa, to w niektórych podmiotach dane osobowe i integralność pacjenta już teraz są tak bardzo „chronione", że nie ma on dostępu do własnej dokumentacji medycznej. Zdarza się, że pacjenci są informowani o braku dostępu wynikającego z troski o ich własne dobro, są to bowiem dane szczególnie wrażliwe. Obserwowany jest także bardzo niski poziom wiedzy pacjentów w tym zakresie, co z kolei prowadzi w podmiotach sektora zdrowia do bagatelizowania zagadnienia i błędnego wniosku, że problem adaptacji do nowych wymagań w Polsce nie istnieje. Połączenie tych dwóch elementów: niewiedzy ze strony pacjentów i bagatelizowania ze strony podmiotów sektora możemy nazwać barierą dostatecznej świadomości interesariuszy systemu. Wpływa ona bezpośrednio na wdrożenie zmian wynikających z nowych przepisów GDPR.

Skonkretyzowana dostępność do danych osobowych w systemie związana jest także z dostępnością do internetowych systemów umawiania wizyt i wystawiania tzw. e-recept. Wśród podmiotów sektora, odsetek gabinetów lekarzy pierwszego kontaktu wykorzystujących komputery osobiste do przechowywania danych medycznych pacjentów oraz do komunikowania się z innymi segmentami systemu opieki zdrowotnej, w tym z płatnikiem (Narodowy Fundusz Zdrowia), stanowi 100%, ale tylko 31% gabinetów lekarzy pierwszego kontaktu korzysta z internetowego umawiana wizyt, a 62% z wystawiania e-recept. Oceniając dostęp do internetowych systemów umawiania wizyt, zauważono, że stosunek podaży do popytu w przypadku wizyt u lekarzy specjalistów czy poważnych zabiegów operacyjnych jest bardzo zbliżony do tego istniejącego dla pokoi hotelowych czy wakacji organizowanych przez biura podróży. Nie ma powodów, dla których pacjenci nie mogliby rezerwować wolnych „miejsc" w dogodnym dla siebie momencie. Nie jest to jednak spotykana praktyka i to nie tylko w Polsce, ale w innych krajach Europy. W 2016 roku tylko trzynaście krajów udostępniło tę usługę znaczącym grupom obywateli, co jest dużym krokiem naprzód (w 2013 r. było to tylko 9 krajów) (EHCI, 2017). Ta dynamika, choć powolna, będzie dodatkowym czynnikiem nakładającym na podmioty systemu obowiązek ochrony danych wrażliwych.

Wśród zakładów opieki zdrowotnej prowadzących leczenie stacjonarne – szpitalne oraz zakładach świadczących specjalistyczne usługi medyczne, przechowywanie danych wrażliwych prowadzone jest za pomocą serwerów, w które wyposażone jest 100% placówek. Wynika to z konieczności zabezpieczenia i przetwarzania znacznie szerszego zakresu informacji w porównaniu do gabinetów lekarzy pierwszego kontaktu. Niestety tu również dostęp do elektronicznego umawiania wizyt i wystawiania e-recept nie jest praktyką powszechną. Jednak na przykładzie tych podmiotów w najbardziej przejrzysty sposób widać zróżnicowanie odpowiedzialności za przechowywanie dokumentacji.

Tabela 1. Podział kontroli i odpowiedzialności pomiędzy usługodawcą a podmiotem zewnętrznym w zależności od modelu przechowywania elektronicznej dokumentacji medycznej

	Model klasyczny	Kolokacja	Hosting
Serwer	Usługodawca	Usługodawca	Podmiot zewn.
Sieć	Usługodawca	Podmiot zewn.	Podmiot zewn.
Środowisko wykonywalne*	Usługodawca	Usługodawca	Usługodawca
Aplikacja	Usługodawca	Usługodawca	Usługodawca
Dane	Usługodawca	Usługodawca	Usługodawca

Źródło: CSIOZ (2016).

2. Bezpieczeństwo danych

Model klasyczny to rozwiązanie, w którym serwer, aplikacja i wszystkie elementy są umieszczone u klienta (typowy przykład to system KS-Somed). Zalety – cała baza i system jest w placówce ochrony zdrowia i ona jest jej właścicielem. Braki Internetu czy inne awarie prądu poza lokalizacją nie wpływają na ciągłość pracy w jednostce. Wady to wyższe koszty uruchomienia z uwagi na zakup i utrzymanie serwerów oraz wyższe koszty zakupu oprogramowania.

Kolokacja stanowi rozwiązanie, w którym serwery jednostki stoją w wynajętych serwerowniach. Zaletą tego rozwiązania jest wyższe bezpieczeństwo dostępu do serwerów (firmy prowadzące tego typu usługi mają przeważnie dużo wyższe zabezpieczenia, kontrole dostępu itp. niż pojedynczy podmiot może zrealizować w jednostce). Zazwyczaj mają też dwa niezależne źródła zasilania oraz przynajmniej 2–3 łącza internetowe od różnych dostawców. W takim przypadku można na serwerach umieścić klasyczne oprogramowanie bądź stworzyć np. prywatną chmurę.

Hosting zaś to rozwiązanie, w którym podmiot nie kupuje serwerów, a jedynie wynajmuje przestrzeń i zasoby od usługodawcy wymagane do zaspokojenia swoich potrzeb w zakresie konkretnego rozwiązania. W takim przypadku najczęściej jednostka korzysta z tzw. rozwiązań chmurowych (można wydzielić również chmurę prywatną, jeżeli usługodawca zapewnia takie rozwiązania). Największą zaletą są najniższe koszty uruchomienia systemu, który nie wymaga zakupu i konfiguracji serwerów, często opłaty za użytkowanie systemów są również miesięczne, co pozwala obniżyć jednorazowe koszty wdrożenia takiego systemu.

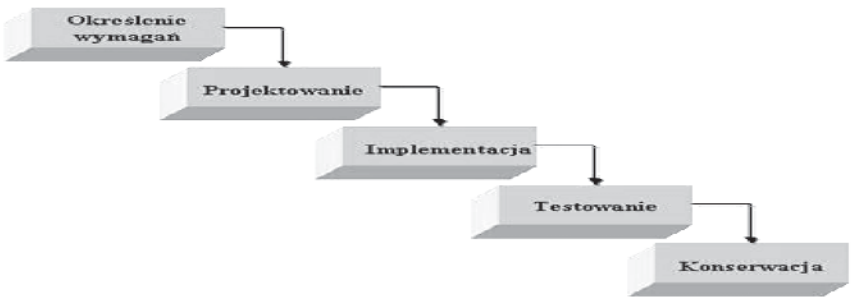
Tabela 2. Przykładowe rozwiązania w omawianych technologiach

Aplikacja	Chmura	Chmura prywatna
KS-SOMED (KAMSOFT)		
KS-PPS (KAMSOFT		
	SERUM (Kamsoft)	SERUM (Kamsoft)
	Mediporta (MEDIPORTA)	
	Eurosoft (EUROSOFT)	
M-MEDICA (ASSECO)		
	OPTIMED24 (COMARCH)	OPTIMED24 (COMARCH)
AXON (AXON)		
Dr Eryk (Erikpol Sp. z o.o.)		

Źródło: opracowanie własne na podstawie rozwiązań systemów ambulatoryjnych (bez systemów szpitalnych).

Obecnie na rynku dostępne są systemy medyczne napisane w stylu klasycznych aplikacji klient–serwer, rozwiązań chmurowych (pracujących najczęściej jako aplikacje sieci www) oraz chmury prywatnej – rozwiązanie chmurowe pozwalające na umieszczenie chmury na serwerach klienta bądź wydzielenie jej jako prywatny obszar w przestrzeni roboczej dostawcy.

Z uwagi na wprowadzenie przez GDPR po raz pierwszy zasad odnoszących się do prywatności i bezpieczeństwa danych o tak silnym umocowaniu w koncepcji modelu cyklu życia systemu informatycznego, należy zauważyć, że najczęściej wymienianym procesem wytwarzania oprogramowania jest model kaskadowy (zwany również modelem wodospadu – *Waterfall*) i model iteracyjny. Wybór procesu zależy od charakteru projektu; w praktyce najlepiej radzą sobie modele, które są hybrydami procesów podstawowych. Sam proces iteracyjny stanowi swego rodzaju modyfikację procesu kaskadowego, zaś inne znane i popularne modele cyklu życia oprogramowania to model spiralny, model V, prototypowanie i wiele innych (Kasprzyk, 2006).



Rysunek 1. Kaskadowy model wytwarzania oprogramowania

Źródło: opracowanie własne.

Analizując zagadnienie bezpieczeństwa danych osobowych w sektorze ochrony zdrowia w oparciu o model cyklu życia systemu informatycznego, za istotną należy uznać wprowadzaną zasadę uwzględniania ochrony danych osobowych – prywatności w fazie projektowania, tzw. *data protection by design* (w skrócie *privacy by design*) oraz *privacy by default* na różnych etapach cyklu życia systemu. Założeniem koncepcji *privacy by design* na etapie projektowania jest wbudowanie funkcji ochrony prywatności w każdy projekt przetwarzający dane osobowe, tak aby były one jego integralną częścią. W tym celu administrator danych musi zebrać wymagania dotyczące bezpieczeństwa przetwarzania danych, zaprojektować oraz zaimplementować odpowiednie środki ochrony (Karg, 2016).

Przepisy GDPR nie zawierają definicji *privacy by design*. Zakres zastosowania zasady należy zatem wprowadzić z charakteru, celu i funkcji normy ustalonej w art. 25 ust. 1 GDPR. Zgodnie z tym przepisem administrator danych: „uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym podobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych" (Rozporządzenie UE 2016/679, 2016). Przykładami środków służących do realizacji tego obowiązku mogą być:

- pseudonimizacja danych osobowych,
- minimalizacja zakresu przetwarzania danych osobowych,
- przejrzystość funkcji przetwarzania danych osobowych,
- umożliwienie osobom, których dane dotyczą, monitorowania przetwarzania danych.

Filozofia *privacy by design* nie ogranicza się jedynie do pierwszego etapu cyklu, obejmuje także regularny przegląd funkcjonowania procesu przetwarzania danych oraz jego składowych elementów (systemów informatycznych, sposobu zbierania zgód, wypełniania obowiązków informacyjnych itp.) w kolejnych etapach cyklu życia systemu. W związku z tym, że proces przetwarzania danych w podmiotach systemu ochrony zdrowia nie kończy się w momencie zakończenia jednej czynności np. rejestracji chorego, dane osobowe będą przetwarzane o wiele dłużej niż do samego momentu zapisu.

2. Nowe zasady

Privacy by default, jako jedna z zasad podstawowych składających się na koncepcję *privacy by design*, zakłada ochronę prywatności jako domyślne ustawienie każdego systemu, którego zmiana może nastąpić wyłącznie przez celowe działanie użytkującego go podmiotu ochrony zdrowia. Bez wątpienia ustawienia domyślne systemu nie są modyfikowane przez większą część użytkujących podmiotów, dlatego tak kluczowe jest zapewnienie wysokiego poziomu bezpieczeństwa w ustawieniach domyślnych syste-

mów. Podmioty, które świadomie chcą zrezygnować z ochrony własnej prywatności, będą musiały podjąć działania w tym kierunku – zmienić ustawienia domyślne systemu. Zasada ta ma zastosowanie szczególnie w chwili przyłączania się podmiotów do systemów. Celem wprowadzenia opisanych regulacji jest podniesienie standardów ochrony danych osobowych i prywatności użytkowników poprzez wprowadzenie elementów ochrony proaktywnej w miejsce reaktywnej. Takie podejście jest próbą uwspółcześnienia strategii ochrony danych osobowych oraz wyjściem naprzeciw aktualnym zagrożeniom prywatności podmiotów przetwarzających dane informatyczne.

Jak wspomniano wyżej, kluczowym elementem tego podejścia jest wkomponowanie problemu ochrony danych osobowych w działania administratora, począwszy od etapu planowania procesu (Karg, 2016). Przykładowo, podmiot sektora opieki zdrowotnej planujący przeprowadzenie konkursu na wyłonienie podwykonawców usług medycznych np. lekarzy specjalistów, będzie zobowiązany do przeprowadzenia oceny, czy zakładane w trakcie konkursu operacje na danych osobowych oraz sposoby ich zabezpieczenia będą zgodne z obowiązującymi przepisami GDPR. Zatem już na tym etapie podmiot sektora powinien rozważyć, na jakiej przesłance zostanie oparty proces przetwarzania danych (jeśli będzie to zgoda, należy przygotować odpowiednio wcześniej jej treść oraz ustalić sposób jej zbierania). Podobnie rzecz będzie się miała z przygotowaniem klauzul obowiązków informacyjnych, zapewnieniem adekwatności przetwarzanych danych oraz ich zabezpieczeniem. W przypadku *privacy by design* chodzi o to, by nie tyle odpowiadać na pojawiające się problemy, co już wcześniej przewidywać najważniejsze z nich i im przeciwdziałać (Wiewiórski, 2014).

Zrozumienie zasad *privacy by design* gwarantuje podmiotom sektora ochrony zdrowia właściwe wdrożenie i prowadzenie procesu przetwarzania danych osobowych z wprowadzanymi przepisami. W tym celu pomocna może być Rezolucja w sprawie prywatności w fazie projektowania przyjęta przez 32. Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności już w 2010 roku (www.giodo.gov.pl). Prywatność w fazie projektowania opiera się na:

- podejściu proaktywnym, nie reaktywnym, zaradczym, nie naprawczym,
- prywatności jako ustawienia domyślnego (tzw. *privacy by default*),
- prywatności włączonej w projekt (tzw. *privacy embedded into design*),
- pełnej funkcjonalności (suma dodatnia, nie suma zerowa),
- ochronie od początku do końca cyklu życia informacji,
- widoczności i przejrzystości,
- poszanowaniu prywatności użytkowników.

Podsumowanie

Wprowadzana przez GRDP zmiana przepisów zmusza podmioty sektora zdrowia do wbudowanie ochrony w architekturę systemu, co poza wyżej opisanymi korzyściami dodatkowo może być bodźcem dla organizacji do zbudowania architektury bezpieczeń-

stwa systemów rozumianej jako próba całościowego podejścia do zabezpieczenia systemów, które obecnie jest niewystarczające. W praktyce realizacja zasady *privacy by design* może być prowadzona poprzez dokonywanie oceny w oparciu o listę kontrolną (*checklist*). Warto przy tym pamiętać, że zasada ta dotyczy zarówno projektowania, jak i realizacji procesu. Sama koncepcja *privacy by design* funkcjonuje obecnie w wielu podmiotach sektora zdrowia, jako mniej lub bardziej sformalizowana dobra praktyka. Każdy z nich przetwarza dane osobowe, po wejściu w życie będzie to dla nich powszechny obowiązek, którego realizacja znajdzie oparcie w przepisach prawa, przewidujących za uchylanie się od *privacy by design* sankcję w postaci kary do 10 000 000 euro (www.giodo.gov.pl). Wprowadzenie zaś tej zasady do działalności podmiotów sektora zdrowia i ich adaptację do nowych rozwiązań należy ocenić pozytywnie – jako praktykę zmierzającą do rzeczywistego przestrzegania przez administratorów zasad przetwarzania danych osobowych, przesuwającą ocenę ochrony danych osobowych do najważniejszych obowiązków każdego z podmiotów.

Literatura

EHCI (2017). A. Bjornberg (red.), *Europejski Konsumencki Indeks Zdrowia Raport 2016*. Health Consumer Powerhouse Ltd.

Karg, M. (2016). *Referent bei der Dienststelle des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2016.* Pobrano z: www.privacy-conference.com.

Kasprzak, R. (2006). Przegląd modeli cyklu życia oprogramowania. Inżynieria oprogramowania. *Software Developer's Journal*, *10*.

Kuczabski, M. (2009). *Medyczne determinanty jakości życia. Bezpieczeństwo obywateli RP jako czynnik jakości życia*. Warszawa: Akademia Obrony Narodowej, Wydział Bezpieczeństwa Narodowego.

Makuchowski, M. (2016). *Komputerowe wspomaganie zarządzania. Cykl życia systemu informatycznego*. Wykłady Politechnika Wrocławska. Pobrano z: mariusz.makuchowski.staff.iiar.pwr.wroc.pl.

OSOZ (2016).

Rezolucja w sprawie prywatności w fazie projektowania przyjęta przez 32. Międzynarodową Konferencję Rzeczników Ochrony Danych i Prywatności (2010). Pobrano z: www.giodo.gov.pl/plik/id_p/2104/j/pl.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. EUR-Lex-32016R0679-EN-EUR-Lex.

Wiewiórski, W. Wywiad z GIODO przeprowadzony przez Fundację Panoptykon. Pobrano z: www.giodo.gov.pl/plik/id_p/2162/j/pl.

IT SYSTEM A HEALTH SECTOR OPERATORS ADAPTATION TO THE NEW UE GENERAL DATA PRIVACY REGULATION

Keywords: security, data protection, privacy law, computer system, health, GDPR

Summary. Introduction of the new European Parliament restrictions concerning data protection of privacy law and free movement of data enforces health sector organizations to implement audit procedures followed by the necessary solutions in the existing computer systems. The new law regulations determine necessity of internal data protection at every stage of system designing process, and the high security level must be imposed on every user as a default rule. This article analyses current solutions to formulate possible consequences and viable adaptation possibilities of health system operators to the expected regulations.

Translated by Mateusz Kuczabski

Cytowanie

Kuczabski, M. (2018). Adaptacja architektury systemów bezpieczeństwa w sektorze ochrony zdrowia do nowych wymagań RODO. *Ekonomiczne Problemy Usług, 2* (131/1), 193–201. DOI: 10.18276/epu.2018.131/1-19.