STUDIA OECONOMICA POSNANIENSIA 2016, vol. 4, no. 12

DOI: 10.18559/SOEP.2016.12.4

Jacek Łuczak

Uniwersytet Ekonomiczny w Poznaniu, Katedra Znormalizowanych Systemów Zarządzania
jacek.luczak@ue.poznan.pl

OCHRONA DANYCH OSOBOWYCH JAKO ELEMENT ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Streszczenie: W artykule zwrócono uwagę na znaczenie informacji oraz konieczność zarządzania jej bezpieczeństwem. Znaczenie informacji wymaga podejścia systemowego, dlatego przybliżone zostały kluczowe definicje i zasady systemu zarządzania bezpieczeństwem informacji. Zwrócono uwagę na liczne wymagania prawne oraz najbardziej znaczące, dotyczące każdej organizacji – związane z bezpieczeństwem danych osobowych. Przedstawione zostały podstawy prawne obowiązujące w Polsce w niniejszym zakresie. Zaprezentowane zostały wyniki badań autora dotyczących zarządzania bezpieczeństwem informacji w zakresie ochrony danych osobowych. Badania zostały przeprowadzone na próbie 130 mikroprzedsiębiorstw, przedsiębiorstw małych i średnich. Badanie ankietowe zostało poszerzone o wywiady pogłębione. W dalszej części przedstawiona została także analiza przypadku dotycząca przedsiębiorstwa z branży informatycznej, dostawcy platform e-learningowych do nauki języka angielskiego. *Case study* dotyczy wybranych elementów systemu zarządzania jakością i bezpieczeństwem informacji, w szczególności w aspektach ochrony danych osobowych.

Słowa kluczowe: system zarządzania bezpieczeństwem informacji, ochrona danych osobowych.

Klasyfikacja JEL: L51.

PERSONAL DATA PROTECTION AS A PART OF INFORMATION SECURITY MANAGEMENT. RESEARCH RESULTS. A CASE STUDY

Abstract: The article stresses the importance of information and the necessity for information security management. The essential role of these issues calls for a system approach; thus, key definitions and principles of information security management have been presented in detail. The paper also takes account of numerous legal requirements, as well as the most significant requirements, as they refer to each organization, relating to personal information security. The legal basis within this scope has also been presented. The article depicts research results linked with information security management within the area of personal data protection. The research was conducted on a sample of 130 micro-, medium-sized and small enterprises. The questionnaire was extended with in-depth interviews. Moreover, the present paper embraces a case study: an IT enterprise, a provider of e-learning platforms for teaching English. The case study is concerned with selected elements of the quality management system and the information security system, particularly in the aspects of personal data protection.

Keywords: Information Security Management System, personal data protection.

Wstęp

Niezależnie od zidentyfikowanych potrzeb i zrozumienia konieczności ochrony i zarządzania bezpieczeństwem informacji, kluczowe jest spełnienie wymagań prawnych. Abstrahując od specyfiki zróżnicowanych działalności, w każdym przypadku ważne są wymagania związane z danymi osobowymi, a zabezpieczenia pod tym względem są ważne dla pracowników, klientów i pracodawcy z uwagi na restrykcje wskazane w ustawie i wiarygodność przetwarzającego dane.

Bardzo niewiele jest działalności zarobkowych (i innych), w których nie ma danych osobowych i nie są one przetwarzane. Dotyczy to wszystkich organizacji, które zatrudniają przynajmniej jednego pracownika. Przetwarzając dane osobowe, należy się stosować do wymagań prawnych. Te nakładają szereg obowiązków, definiują istotne ograniczenia. Spełnienie wymagań jest kosztowne i ogranicza łatwość prowadzenia działalności gospodarczej. Przy tym jednak stwierdzenie, że prowadzenie biznesu jest łatwiejsze bez jakichkolwiek ograniczeń, jest demagogiczne, jak to określa Kępa [2015, s. 11].

Spełnienie wymagań prawnych jest kluczowym aspektem zarządzania bezpieczeństwem organizacji, istotnym również w innych rozwiązaniach

w ujęciu systemowym. Z uwagi na rozpoznawalność rynkową dobrym tego przykładem jest SZBI (system zarządzania bezpieczeństwem informacji) zgodny z międzynarodowym standardem ISO/IEC 27001.

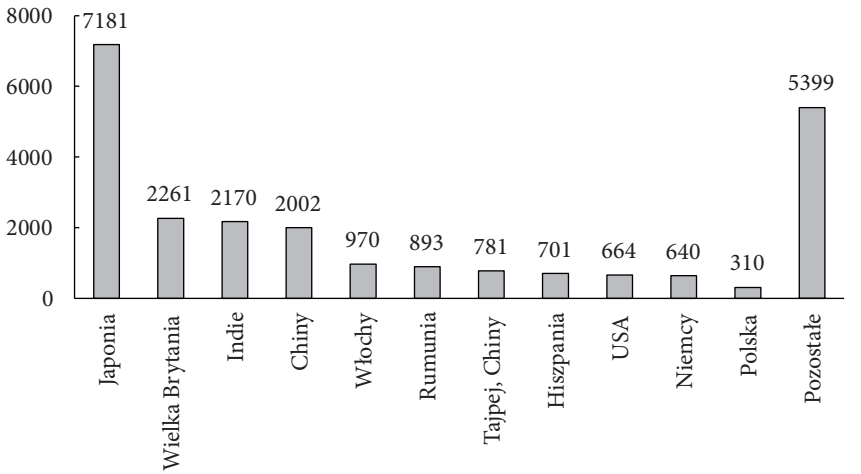
W artykule podjęty został temat zapewnienia bezpieczeństwa informacji personalnych jako aspekt systemu zarządzania bezpieczeństwem informacji w szerszym rozumieniu. Przedstawione zostały kluczowe wymagania w ww. zakresie, wyniki badań autora odnoszących się do ochrony danych personalnych oraz *case study* organizacji IT. Celem nadrzędnym artykułu jest zwrócenie uwagi na nieprzygotowanie, a często nieświadomość organizacji w zakresie aspektów prawnych dotyczących ochrony danych osobowych.

1. Systemowe zarządzanie bezpieczeństwem informacji

Bezpieczeństwo w potocznym znaczeniu jest rozumiane jako stan niezagrożenia i od wieków jest pożądane w wielu sferach aktywności człowieka [Białas 2007, s. 27]. W odniesieniu do bezpieczeństwa informacji jest związane z niezakłóconym funkcjonowaniem procesów organizacji. Mottord i Whitman określają bezpieczeństwo informacji jako „jakość stanu organizacji wolnej od zagrożeń związanych z bezpieczeństwem informacji" [Mottord i Whitman 2008, s. 4]. Peltier [2002] zwraca uwagę, że celem ochrony informacji jest ochrona wartościowych dla organizacji zasobów – informacji, ale także środowiska tworzonego przez *hardware* i *software* [Peltier 2002, s. 1].

Definiując bezpieczeństwo informacji, wskazuje się na szereg aspektów, przede wszystkim poufność, autentyczność, dostępność, integralność, rozliczalność, niezawodność [Białas 2007, s. 34). Whitman i Mottord [2008] wskazują także na prywatność jako jeden z aspektów wymagających ochrony właśnie z uwagi na związek z daną osobą. Informacje personalne to aktywa informacyjne mające swoją wrażliwość, którą definiuje się jako miarę ważności przypisaną informacji przez jej autora lub dysponenta w celu wskazania konieczności jej ochrony [Białas 2007, s. 37].

Wielu autorów wskazuje na zasadność wdrożenia systemu zarządzania bezpieczeństwem informacji (w ramach konkretnego modelu), a przynajmniej na wykorzystanie kluczowych elementów, powszechnie uznawanych za niezbędne dla zapewnienia bezpieczeństwa informacji (m.in. polityka, zarządzanie ryzykiem, zarządzanie zabezpieczeniami, zarządzanie incydentami) [m.in. Calder 2005, s. 23; Hunter 2001, s. 9]. Uniwersalną rolę w tym zakresie odgrywa międzynarodowy standard ISO/IEC 27001. W 2014 r. odnotowano 23 972 certyfikaty na świecie, a w Polsce 310 [ISO Survey 2015].



Rysunek 1. Liczba certyfikatów ISO/IEC 27001 na świecie (2014 r.)
Źródło: [ISO Survey 2015]

Wielu autorów sugeruje, że dla zapewnienia ciągłości procesów konieczne jest zarządzanie informacją w ujęciu systemu bezpieczeństwa informacji [por. Osborn 2006, s. 21–24], choć za główny motyw uzyskiwania certyfikatów wskazuje się wymagania rynkowe, co jest zrozumiałe. Z tym jednak związany jest paradoks, bowiem właśnie certyfikowane organizacje odnotowują wzmożoną aktywność w zakresie nieautoryzowanych prób dostępu do zasobów informacyjnych (w systemach informatycznych) [por. Łuczak i Tyburski 2010, s. 71]. Przy tym należy zwrócić uwagę na przytoczony standard jako zbiór dobrych praktyk, o najbardziej uniwersalnym wymiarze (nie tylko dla organizacji IT, może w najmniejszym stopniu przystających do organizacji IT). Obejmuje on wszystkie znaczące elementy związane z zarządzaniem bezpieczeństwem informacji, w tym także z bezpieczeństwem teleinformatycznym.

Podkreślane są różne kluczowe aspekty systemowego zarządzania bezpieczeństwem informacji. Humphreys [2007] wskazuje na konieczność oparcia systemu na szacowaniu ryzyka w sposób najbardziej adekwatny do specyfiki organizacji [Humphreys 2007, s. 1; Shostack i Stewart 2008, s. 64–65.]

Organizacje i ich rozwój są zależne od nieustannego zasilania w informację, która najczęściej jest już w formie elektronicznej, dlatego istotą bezpieczeństwa informacji jest bezpieczeństwo teleinformatyczne [Białas 2007; Axelrod, Bayuk i Schutzer 2009]. Wątpliwości nie pozostawia konieczność

zgodności z prawem, np. w przypadku USA oznacza to uwzględnienie SoX (Sorbanes Oxley) znanego także jako the Public Company Accounting Reform and Investor Protection Act of 2002, GLBA (Gramm-Leach-Bliley Act) czyli Gramm-Leach-Bliley Financial Services Modernization Act, Base II i wielu innych.

Organizacje prowadzące działalność w Polsce powinny się skoncentrować na co najmniej kilku aktach prawnych związanych z ochroną informacji, przy czym – niezależnie od specyfiki danej organizacji – do najważniejszych zdecydowanie należą regulacje dotyczące ochrony danych osobowych.

Pośród wielu innych obszarów systemu zarządzania informacją wymieniane są:

- świadomość dotycząca zarządzania bezpieczeństwem informacji,
- podział ról (odpowiedzialności i uprawnień) w zakresie bezpieczeństwa informacji,
- zarządzanie incydentami,
- etyka w zarządzaniu informacją,
- optymalizacja rozwiązań w zakresie zarządzania informacją z wartościami społecznymi,
- priorytetowość aspektów bezpieczeństwa i podejście systemowe,
- ciągłe doskonalenie [Humphreys 2007, s. 14].

W przypadku decyzji o wdrożeniu i certyfikacji SZBI, zgodnie z międzynarodową normą ISO/IEC 27001, organizacja powinna ustanowić, wdrożyć, utrzymać i ciągle doskonalić system zarządzania bezpieczeństwem informacji [ISO/IEC 27001, p. 4.4, s. 8] – to wymaganie ogólne, jednak niepozostawiające żadnej wątpliwości co do konieczności spełnienia wymagań standardu ISO/IEC 27001. W praktyce oznacza to konieczność interpretacji wszystkich wymagań, ich spełnienie w sposób adekwatny do specyfiki organizacji. Istotną rolę w tym względzie odgrywają wymagania prawne, które regulują poziom ochrony danych o charakterze wrażliwym. Pośród nich ważne są dane personalne. Bezpieczeństwo danych to aspekt często niedostatecznie uświadomiony w organizacji, tak z uwagi na jej znaczenie, jak również wymagania dotyczące ich ochrony. Niewystarczającą świadomość w tym zakresie mają zarówno pracodawcy, jak i pracownicy, współpracownicy, klienci, których dane personalne stanowią ich własność i muszą być zabezpieczone. Jest to niezwykle ważne nie tylko z uwagi na wymagania prawne w tym zakresie, ponieważ ochrona danych to także wiarygodność rynkowa wobec kontrahentów. Dane wrażliwe pod tym względem odgrywają rolę szczególną, a dane osobowe – niezwykle ważną.

Fundamentem w zakresie systemowego zarządzania danymi jest spełnienie wymagań prawnych, podobnie zresztą jak w przypadku innych systemów znormalizowanych. Aspekt ten powinien stanowić w każdym przypadku podstawę rozwiązań systemowych. Temat jest tym bardziej istotny, że – jak wskazują badania – organizacje nie są świadome wymagań oraz nie mają kompetencji w zakresie zapewnienia bezpieczeństwa danych personalnych na poziomie prawa UE. Ze względów formalnych w zasadzie bez znaczenia wobec obowiązków wynikających z ustawy jest system zarządzania bezpieczeństwem informacji w wymiarze ISO/IEC 27001. Stanowi on jednak doskonałą podstawę dla zapewnienia bezpieczeństwa danych osobowych. Warto zwrócić uwagę, że trudność rzeczywistą stanowi spełnienie wymagań ustawowych bez wcześniej wdrożonego znormalizowanego systemu, oczywiście najlepiej dotyczącego bezpieczeństwa informacji. W powiązaniu z wymaganiami ISO/IEC 27001 można mówić o bardzo dobrych podstawach dających szansę na skuteczne zapewnienie bezpieczeństwa danych personalnych.

Praktyczne aspekty zarządzania związane ze spełnieniem wymagań prawnych stanowią problem dla przedsiębiorców. Każdy pracownik, klient czy użytkownik, którego dane zostały zarejestrowane, powinien mieć gwarancję bezpieczeństwa swoich danych.

2. Bezpieczeństwo danych osobowych

Identyfikacja i spełnienie wymagań prawnych to obowiązek każdego przedsiębiorcy. W odniesieniu do systemowego zarządzania bezpieczeństwem informacji to kluczowy aspekt, który należy uwzględnić przy doborze zabezpieczeń (uwzględnieniu w deklaracji stosowania), szacowaniu ryzyka itd. Wiele aktów prawnych dotyczy większej czy mniejszej grupy organizacji, na przykład w zakresie ochrony informacji niejawnych, własności intelektualnej czy w sferze handlu elektronicznego i usług oraz konkretnych sferach działalności – np. usługach bankowych, ubezpieczeniowych. Niemal wszystkie organizacje przetwarzają dane osobowe, dlatego muszą spełniać adekwatne wymagania, określone na poziomie ustawy i rozporządzeń.

Obowiązująca ustawa o ochronie danych osobowych pochodzi z 1997 r., choć była już kilkanaście razy nowelizowana (Dz.U. 2015, poz. 2135 z późn. zm.). Pierwotnie była implementacją dyrektywy UE (95/46/WE), która zobowiązywała Polskę do wskazania sposobu osiągnięcia określonych w niej celów. Największe zmiany nastąpiły w 2004 r. w związku z przystąpieniem

Polski do UE. Ponadto bardzo istotne są rozporządzenia dotyczące dokumentacji oraz wymagań dotyczących systemów informatycznych określonych w Rozporządzeniu 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 i systemy teleinformatyczne służące do przetwarzania danych osobowych [Rozporządzenie 2004].

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady Europy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych zostanie zastąpiona rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Rozporządzenie będzie obowiązywało bezpośrednio w krajach członkowskich, stanowiąc element systemu prawnego wszystkich członków UE. To spowoduje całkowitą harmonizację prawa w omawianym zakresie w ramach całej UE i swobodnego przepływu danych osobowych.

Jednocześnie należy zwrócić uwagę na dyrektywę Parlamentu Europejskiego i Rady Europy w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych, tym bardziej że reguły zawarte w projekcie wypełniają lukę w polskich przepisach prawa (GIODO).

Ustawa o ochronie danych osobowych stawia wymagania, które stanowią ograniczenia dla przedsiębiorców, równe dla wszystkich prowadzących działalność; nie pozwala ona na podejmowanie pewnych działań, które byłyby efektywne i wygodne z punktu widzenia osoby prowadzącej działalność nie tylko gospodarczą, ale też np. społeczną. Ustawa bowiem pozwala na wykorzystanie danych osobowych na potrzeby prowadzenia działalności gospodarczej, ale tylko w takim zakresie, który jest niezbędny i adekwatny do celu, jaki ma zostać osiągnięty[1]. Przy tym stosowanie wymagań to zwiększenie wiarygodności wobec klientów oraz uczciwe postępowanie wobec pracowników. Za stosowaniem wymagań przemawiają także względy pragmatyczne, bowiem tego typu dane, niezależnie od restrykcji, powinny być chronione, chociażby ze względu na ich wartość dla konkurencji. Często zabezpieczenia ustanowione dla ochrony baz z danymi osobowymi są wyznacznikiem poziomu bezpieczeństwa dla innych informacji. Warto

[1] Wypowiedź generalnego inspektora ochrony danych Wojciecha Rafała Wiewiórowskiego; posiedzenie nr 8 w dn. 17.02.2012 r.

podkreślić, że zagadnienia związane z przetwarzaniem baz danych są regulowane w ponad 100 aktach normatywnych. Kępa [2015] zwraca uwagę, że jedne coś dopuszczają, inne zabraniają, jeszcze inne zwracają uwagę na szczególne przypadki. A przy tym nieprzestrzeganie prawa pod tym względem jest niejednokrotnie ścigane z urzędu i grożą za to rozmaite kary.

Spotkać można skrajne opinie związane z restrykcyjnymi przepisami prawa w omawianym zakresie. Bez wątpienia łatwiej jest prowadzić działalność gospodarczą, na którą nie są nałożone wymagania i grożące restrykcje. Jednocześnie taka swoboda ma charakter iluzoryczny, bowiem w żadnym razie nie gwarantuje zaufania w relacjach biznesowych. Spełnienie wymagań ustawy to konieczność, określone koszty wydają się adekwatne do celu, jaki powinien zostać osiągnięty. Cel ten to oczywista ochrona danych osobowych każdego z nas. Jednak „ustawa pozwala na wykorzystywanie danych osobowych dla potrzeb prowadzenia działalności gospodarczej, ale tylko w takim zakresie, który jest niezbędny i adekwatny do celu, który ma zostać osiągnięty" (GIODO).

Konstytucja RP określa, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym [Konstytucja RP, art. 47]. Prawa do prywatności zostały przybliżone także w artykule 51 Konstytucji, w którym zwraca się uwagę m.in. na fakt, że wyłącznie ustawa może zobowiązać kogokolwiek do ujawnienia danych osobowych, a ich właściciel musi mieć zagwarantowane prawo wglądu, modyfikacji i ich usunięcia. Zmiany i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Ustawa o ochronie danych osobowych w art. 1 wskazuje, że każdy ma prawo do ochrony dotyczących go danych osobowych, a obywatele mają szereg praw, m.in.:

- osoba, której dane dotyczą, ma prawo sprawować kontrolę nad tym, kto i jakie dane jej dotyczące przetwarza;
- dane mogą być przetwarzane tylko zgodnie z prawem, w określonym czasie i celu;
- do informacji – kto i w jakim zakresie przetwarza dane;
- do sprostowania, uzupełnienia czy usunięcia danych.

Prawa do prywatności są wzmocnione przez obowiązek rejestracji zbiorów danych osobowych w zasobach GIODO. Jednak ostatnie nowelizacje zakładają, że w przypadku powołania administratora danych osobowych to właśnie ABI utrzymuje rejestr (operator danych nie musi zgłaszać zbiorów). Artykuł 23 ustawy zwraca uwagę, że przetwarzanie jakichkolwiek danych osobowych jest możliwe tylko wtedy, gdy spełniona została co

najmniej jedna przesłanka legalności przetwarzania danych. Jedna z kluczowych to wyrażenie na to zgody przez właściciela danych. Szczególnej ochronie podlegają tzw. dane wrażliwe (art. 27), które są szczególne wobec prywatności osoby (np. informacje o zdrowiu, kodzie genetycznym, preferencjach seksualnych). Ustawa zwraca także uwagę na bezpieczeństwo teleinformatyczne, dlatego poza udokumentowaną polityką bezpieczeństwa danych personalnych konieczna jest także pisemna instrukcja zarządzania systemem informatycznym.

3. Świadomość dotycząca wymagań związanych z ochroną danych osobowych

W okresie 10.2015 r.–01.2016 r. przeprowadzone zostały przez autora badania dotyczące zarządzania bezpieczeństwem informacji. Problem badawczy określony przez autora koncentrował się na podejściu małych i średnich przedsiębiorstw do rozwiązań w zakresie bezpieczeństwa informacji. Jednym z podjętych w badaniu aspektów jest ocena świadomości, motywacji oraz rozwiązań w zakresie ochrony danych osobowych.

Badaniu poddanych zostało 130 przedsiębiorstw produkcyjnych i usługowych z różnych branż. Badanie przeprowadzono za pomocą ankiety internetowej poszerzonej o wywiady bezpośrednie przeprowadzone w kilku z badanych przedsiębiorstw.

Próba badawcza to 130 przedsiębiorstw z województwa wielkopolskiego, wnioskowanie zostało przeprowadzone na podstawie 48 prawidłowo wypełnionych ankiet, rezultatów wywiadów oraz badań uczestniczących w przedsiębiorstwach w charakterze konsultanta i audytora.

Teza przyjęta w badaniach, odnosząca się do omawianej części badań, koncentruje się na wymaganiach określonych w ustawie o ochronie danych osobowych. Jedna z hipotez cząstkowych zakłada, że w większości przypadków przedsiębiorcy nie mają świadomości i wiedzy w zakresie wymagań dotyczących ochrony danych personalnych, nie spełniają wymagań. W konsekwencji narażają właścicieli danych, a siebie na konsekwencje związane z odpowiedzialnością określoną w ustawie oraz konsekwencje rynkowe, dotyczące przede wszystkim wiarygodności.

W badaniu wzięło udział 21 małych przedsiębiorstw, 14 średniej wielkości oraz 13 mikroprzedsiębiorstw. W badanej próbie siedem posiadało certyfikowany system zarządzania jakością (np. ISO 9001 lub ISO 20000-1), trzy z nich były certyfikowane na zgodność z ISO 14001, a dwie po-

siadają system zarządzania bezpieczeństwem informacji zgodny z ISO/IEC 27001.

Zaskakujące są odpowiedzi na kluczowe pytanie o przetwarzanie danych osobowych. Aż 15 organizacji zaprzeczyło przetwarzaniu danych, dziewięć stwierdziło, że nie wie, a nawet nie połowa badanych (20) potwierdziła. Przy czym już 40 respondentów potwierdziło, że przetwarza bazy danych pracowników, 36 klientów, a trzynastu w odniesieniu do danych użytkowników produktów. W tym miejscu można zwrócić uwagę na fakt, że respondenci nie posługują się prawidłowo definicjami, jakie zostały przyjęte w ustawie, w szczególności w odniesieniu do przetwarzania danych osobowych, np. nie uznają, że archiwizowanie to także element przetwarzania danych. Ponadto w bardzo wielu przypadkach respondenci nie potrafili rozdzielić sytuacji, kiedy organizacja, którą reprezentują, jest operatorem danych, a kiedy przetwarza dane na podstawie upoważnienia. Okazało się także, że w zdecydowanej większości przypadków respondenci, którzy przetwarzają dane, nie mają właściwie przygotowanego, pisemnego upoważnienia. Podobnie upoważnienia dla pracowników (i ewentualnie innych osób) bezwzględnie nie spełniają wymagań, są nieaktualne, nieprecyzyjne.

Sześciu z respondentów wskazuje na powołanie administratora bezpieczeństwa informacji i w tych przypadkach precyzyjnie zostały ustalone odpowiedzialności i uprawnienia, które obejmowały wymagania prawne. Powołanie ABI nie jest obowiązkowe, przy czym jeżeli nastąpi, to przejmuje on szereg obowiązków administratora. Konieczne jest zatem nadanie mu adekwatnych uprawnień.

Trzydziestu respondentów potwierdziło, że określiło jednoznacznie role, odpowiedzialności i uprawnienia w zakresie zapewnienia bezpieczeństwa informacji. Przy tym jednak aż w 35 przypadkach respondenci wskazali, że kluczową rolę pełni kierownictwo, w siedmiu przypadkach powołany został ABI. Ponad 25% respondentów nie określiło odpowiedzialności w tym zakresie. Wyniki nie są jednoznaczne, a pewną wskazówką przy interpretacji wyników jest niezwykle niski stopień świadomości w zakresie wymagań dotyczących bezpieczeństwa danych personalnych. Zaledwie połowa respondentów wskazała na Ustawę jako podstawowy zbiór wymagań, a badania pogłębione dowiodły braku wiedzy dotyczącej jej nowelizacji. Czwarta część respondentów zadeklarowała, że nie wie, jakie są wymagania, pozostali badani wskazali niewłaściwe zbiory wymagań. Wyniki badania są zaskakujące, zważywszy że ustawa przewiduje odpowiedzialność karną. Skoro na 44 przypadki zaledwie w siedmiu powołany został administrator bezpieczeństwa informacji, to należałoby oczekiwać wielu przypadków

zgłoszenia baz do GIODO. Ale deklaruje to zaledwie ośmiu respondentów, choć jednocześnie w czasie wywiadu bezpośredniego często nie potrafią oni wyjaśnić meandrów wymagań i wyłączeń.

Przytaczając wyniki badań, konieczne jest zwrócenie uwagi na fakt, że zgodnie z deklaracją niemal połowa respondentów (20) transferuje dane poza granice Polski, w tym 12 do UE, a osiem do państw trzecich. Przy tak niskiej świadomości respondentów w zakresie wymagań można wysnuć wniosek o bardzo prawdopodobnych niezgodnościach w tym zakresie.

Jednoznacznie można ocenić odpowiedzi udzielone na pytanie o posiadanie niezbędnej dokumentacji. Tylko 10 respondentów zadeklarowało, że posiada wymaganą politykę bezpieczeństwa danych personalnych oraz instrukcję sieci IT. 21 odpowiadających stwierdziło, że wymaganie ich nie dotyczy, a 15 – że nie ustanowiło wymienionych dokumentów. Jeszcze bardziej zastanawiający jest rezultat analizy dokumentów tego typu. Najczęściej to tylko formalne spełnienie wymagań, które jest przygotowane według wzoru, który nie został nawet w najmniejszym stopniu dostosowany do realiów danej organizacji. Najczęściej to przejaw całkowitej ignorancji. W pojedynczych zaledwie przypadkach fakt ten wynika z uregulowania zasad nadzoru nad danymi personalnymi w dokumentacji systemu zarządzania bezpieczeństwem informacji.

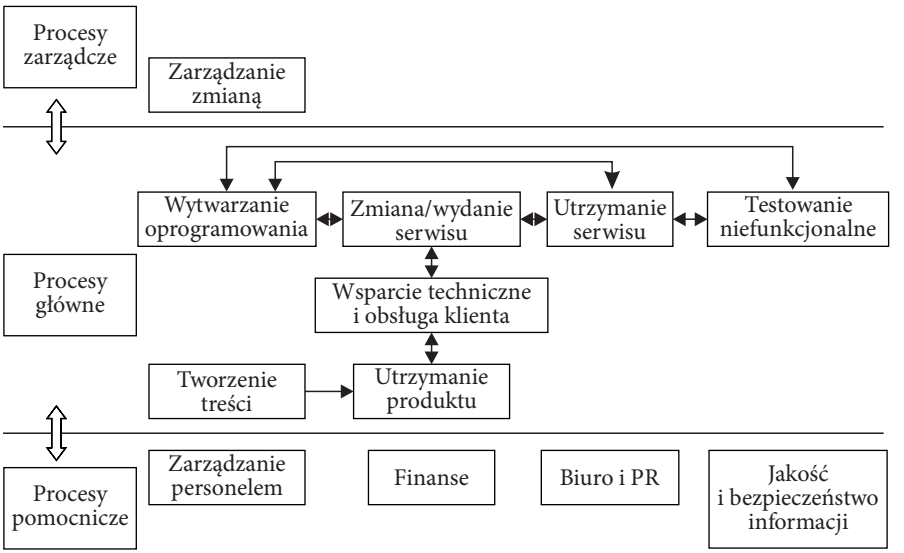
4. Ochrona danych osobowych jako element zintegrowanego systemu zarządzania jakością i bezpieczeństwem informacji. *Case study*

W niniejszej części zostały scharakteryzowane wybrane aspekty systemu zarządzania bezpieczeństwem danych osobowych w organizacji usługowej IT, zlokalizowane w Polsce.

4.1. Charakterystyka organizacji

Organizacja jest uznanym i dużym dostawcą usług e-learningowych do nauki języka angielskiego. Posiada oddziały w Anglii, USA, Chinach i Polsce – tzw. *software houses* (producentów oprogramowania) oraz centra o charakterze „*research and development*". Jeden z kluczowych oddziałów jest zlokalizowany w Polsce, odpowiada przede wszystkim za rozwijanie głównej platformy softwareowej (jak również innych produktów) oraz świadczenie wsparcia dla klientów – w formie szkoleń i instruktarzy, a także *call centre*.

Specyfikę organizacji najlepiej oddaje jej mapa procesów opracowana w ramach systemu zarządzania jakością (ISO 20000-1) oraz zarządzania bezpieczeństwem informacji (ISO/IEC 27001), jak również wobec postawionych celów związanych ze standaryzacją i pomiarem efektywności.



Rysunek 2. Mapa procesów dostawcy usług e-learningowych

Kluczowe procesy stanowią rozwiązania informatyczne, które w efekcie są związane z kreowaniem, utrzymaniem i rozwojem platform e-learningowych. Jest to grupa procesów: wytwarzanie oprogramowania, zmiana/wydanie serwisu, utrzymanie serwisu oraz testowanie niefunkcjonalne.

Główne procesy budowane są przez procesy: tworzenia treści, utrzymania produktu oraz wsparcia technicznego i obsługi klienta. Tworzenie treści zapewnia konieczne ćwiczenia, testy, materiały do nauki języka angielskiego, a wsparcie dotyczy działań na rzecz udostępniania usług użytkownikom, ale także działań analitycznych, związanych z rozwojem produktów.

Ponadto określony został proces o charakterze nadrzędnym – zarządzanie zmianą, który łączy w sobie konieczność respektowania wytycznych obowiązujących w całej korporacji oraz zarządzanie w ramach organizacji w Polsce, realizowanej zgodnie z koncepcją *agility path* oraz *scram*.

4.2. Zarządzanie jakością, bezpieczeństwem informacji oraz ochrona danych osobowych

W organizacji jednoznacznie podzielono role w zakresie systemu zarządzania jakością, bezpieczeństwem oraz ustawową odpowiedzialność związaną z ochroną danych osobowych. Kluczową rolę w tym zakresie odgrywa *quality and information security manager*, który jednocześnie jest administratorem bezpieczeństwa informacji. Ostatnia funkcja wynika z mocy ustawy, jednak nie jest obowiązkowa. W praktyce zatem ww. osoba odpowiada wyłącznie przed zarządem za wdrożenie, utrzymanie i rozwój systemu zarządzania oraz przejęła zdecydowaną większość obowiązków organizacji (operatora danych osobowych).

W ramach systemu zarządzania funkcjonują także:

– właściciele procesów – odpowiedzialni za zarządzanie danym procesem, począwszy od dokumentacji, a kończąc na opomiarowaniu poprzez zaproponowane KPIs (*key performance indicators*);
– właściciele baz danych osobowych – wyznaczeni pracownicy, którzy odpowiadają za bazy danych zawierające dane osobowe, w szczególności za dokonywanie uzgodnień z ABI dotyczących zmian w zakresie zbierania danych i struktury bazy; są oni także odpowiedzialni za zgłaszanie osób, które muszą zostać upoważnione do przetwarzania danych;
– członkowie forum bezpieczeństwa – odpowiadają za szacowanie ryzyka dotyczącego bezpieczeństwa informacji, uzgadnianie i akceptację planów postępowania z ryzykiem. Forum bezpieczeństwa przygotowuje także przegląd zarządzania, który odbywa się etapowo w ramach cotygodniowych spotkań kierownictwa.

Quality and information security manager w praktyce jest koordynatorem bardzo rozproszonych działań, umiejscowionych w ramach poszczególnych procesów. Zgodnie z przyjętymi założeniami zadania przez niego realizowane znalazły się w grupie dziesięciu zadań priorytetowych dla rozwoju organizacji:

– podejście procesowe i dokumentacja SZBI – zakłada weryfikację mapy procesów i podporządkowanie jej założeniom optymalizacji i pomiaru efektywności z uwagi na fakt, że dotychczasowa podporządkowana była wyłącznie spełnieniom wymagań norm stanowiących podstawę systemu;
– zarządzanie ryzykiem – rezygnacja z dotychczasowej metody (MEHARI), bowiem nie jest zrozumiała, w efekcie plany postępowania z ryzykiem oparte na rezultatach szacowania ryzyka nie są rzeczywistym, czytelnym elementem doskonalenia systemu;

– zarządzanie danymi osobowymi – z uwagi na uświadomienie ilości danych przetwarzanych w roli operatora danych osobowych oraz powierzonych przez siedzibę główną organizacji oraz z uwagi na powszechny transfer danych poza strefę UE.

Niezależnie realizowane są aktywności dotyczące utrzymania systemu, związane z audytowaniem, zarządzaniem incydentami, wykonaniem zadań z planu postępowania z ryzykiem itd.

Wymagania realizowane w zakresie ochrony danych osobowych są całkowicie zintegrowane z systemem zarządzania jakością i bezpieczeństwem informacji, co gwarantuje odpowiedzialność jednej osoby bezpośrednio przed zarządem. Kluczowe dokumenty związane z nadzorowaniem danych osobowych to polityka ochrony danych osobowych oraz instrukcja nadzoru nad siecią informatyczną – opracowane w ramach procesu zarządzania jakością i bezpieczeństwem informacji, przy czym istotne jest odwoływanie się w nich do wielu dokumentów systemowych.

W omawianej firmie model dokumentacji jest opisany na dwóch poziomach. Pierwszy poziom to charakterystyka procesów w postaci tzw. *process books*, które odwołują się do polityki oraz instrukcji. Zgodnie z uzgodnioną zasadą uwzględniają one dokumenty centralne (emitowane przez właściciela w Wielkiej Brytanii) i nie są z nimi sprzeczne. Kluczowe dokumenty dotyczące ochrony danych personalnych przywołują przede wszystkim:

– deklarację stosowania, która określa wszystkie zabezpieczenia stosowane w organizacji, w tym dotyczące sieci IT oraz w szerszym ujęciu teleinformatyczne;
– instrukcje związane z zapewnieniem ciągłości działania oraz planami DRP (*disaster recovery plan*);
– instrukcje postępowania z incydentami dotyczącymi bezpieczeństwa informacji;
– katalog usług obejmujący minimalne parametry świadczenia usług, w tym SLA (*standard level agreement*);
– instrukcje monitorowania i oceny skuteczności zabezpieczeń informatycznych.

Zgodnie z wymaganiami ABI odpowiada za utrzymywanie baz danych obejmujących dane personalne. Są one wyspecyfikowane w nadzorowanym pliku jako tzw. jawny rejestr. Każda baza jest scharakteryzowana poprzez podanie jej nazwy, głównego użytkownika, listy osób upoważnionych do przetwarzania danych osobowych, wskazanie administratora bazy danych, identyfikację celu przetwarzania danych, charakterystyki zbiorowości, jaką dane baza zawiera, rodzaju danych zbieranych w bazie oraz struktury da-

nych. Ponadto szereg innych charakterystyk bardziej szczegółowych uzupełnia rejestr.

W rejestrze jawnym określone zostały tylko bazy wymagane przez ustawę (jest ich 12), w niniejszej organizacji dotyczy to sytuacji, kiedy jest ona operatorem danych osobowych, a bazy zawierają dane użytkowników oprogramowania. Bazy są utrzymywane dla celów analitycznych oraz świadczenia wsparcia w czasie eksploatacji.

Drugi rodzaj rejestru ma przeznaczenie wewnętrzne, zawiera bazy (w liczbie 37), w przypadku których omawiana firma przetwarza dane powierzone (przez jednostkę nadrzędną, na podstawie umowy) lub są to bazy pracowników i współpracowników.

Niezwykle trudne jest zapewnienie skutecznego nadzoru nad upoważnieniami, bowiem dotyczy to niemal 50 baz danych oraz niemal 250 pracowników, współpracowników, często spoza firmy, czy strefy UE.

Nadzór nad skutecznością ZSZiBI jest realizowany przez audyty wewnętrzne oraz kontrole ABI w zakresie ochrony danych osobowych i formalnego raportowania, do jakiego jest zobowiązany. Standard ochrony danych osobowych wyznacza poziom zarządzania bezpieczeństwem wszystkich danych, co początkowo okazywało się zbyt restrykcyjnym podejściem. Jednak świadomość dotycząca wielkości baz (kilka milionów osób), incydenty związane z nieautoryzowanymi dostępami (np. Wikileaks) spowodowały radykalizację podejścia właścicieli organizacji.

Zakończenie

Bezpieczeństwo informacji jest ważnym aspektem zarządzania każdą organizacją. Zważywszy na jej specyfikę, może mieć charakter krytyczny z uwagi na wartość rynkową – decydować o przewadze konkurencyjnej. Dane personalne natomiast w każdym przypadku muszą być chronione, chociażby z uwagi na wymagania określone w aktach prawnych. Odpowiedzią na potrzeby rynkowe czy nawet tylko wymagania są rozwiązania systemowe w zakresie zarządzania bezpieczeństwem danych. Mogą one być oparte na rozpoznawalnym, międzynarodowym standardzie ISO/IEC 27001. Wdrażając, utrzymując i rozwijając system zarządzania bezpieczeństwem informacji, należy spełniać kilka grup wymagań. Warunkiem koniecznym ustanawiania i wdrażania skutecznego systemu zarządzania bezpieczeństwem informacji jest spełnienie wymagań prawnych, w tym dotyczących ochrony danych osobowych. Wyniki badań przeprowadzonych przez autora na pró-

bie 130 przedsiębiorstw wskazują na bardzo niską świadomość kadry zarządzającej w odniesieniu do konieczności ochrony danych personalnych, co może skutkować niedostateczną dbałością o prawa ich właścicieli. Krótkowzroczność pod tym względem przejawia się nawet w niewiedzy dotyczącej podstaw prawnych, ustanowienia i udokumentowania wymaganej polityki i instrukcji oraz utrzymywania rejestrów baz danych. Posługując się terminologią standardu ISO/IEC 27001 (czy innych norm stanowiących podstawę systemów znormalizowanych), są to niezgodności krytyczne; przy czym w tym przypadku przedstawicielom operatora danych osobowych grozi odpowiedzialność karna i utrata wiarygodności rynkowej.

Bibliografia

Axelrod, C.W., Bayuk, J.L., Schutzer D. (eds.), 2009, *Enterprise Information, Security and Privacy*, Artech House, Norwood.

Białas, A., 2007, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WNT, Warszawa.

Calder, A., 2005, *A Business Guide to Information Security*, Kogan Page, London.

Humphreys, E., 2007, *Implementing the ISO/IEC 27001Information Security Management System Standard*, Artech House, Norwood.

Hunter, J.M.D, 2001, *An Information Security Handbook*, Springer, London.

ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements.

ISO Survey 2015, Executed summary, International Standards Organization.

Kępa, L., 2015, *Ochrona danych osobowych w praktyce*, Difin, Warszawa.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U., nr 78, poz. 483.

Łuczak, J., Tyburski, M., 2010, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu, Poznań.

Mottord, H.J., Whitman, M.E., 2008, *Management of Information Security*, 2nd ed., Thomson, Boston.

Osborn, M., 2006, *How to Cheat at Managing Information Security*, Syngress, Rockland.

Peltier, T.R., 2002, *Information Security Policies, Procedures and Standards*, Auerbach Publications.

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.

Shostack, A., Stewart, A., 2008, *A New School of Information Security*, Pearson Education.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U., nr 133, poz. 883, z późn. zm.