EBIB Biuletyn EBIB, nr 1 (163)/2016,
Prywatność w bibliotece
Artykuł

Sylwia Czub-Kiełczewska
Instytut Książki

Przepisy o ochronie danych osobowych – jak biblioteki sobie z tym radzą?

Streszczenie: Autorka opisuje swoje doświadczenia ze szkoleń, jakie przeprowadza dla bibliotekarzy. Sygnalizuje tematykę szkoleń, trudności, jakie wynikają z przyswajania wiedzy, przytacza przepisy, które powinny być w bibliotekach przestrzegane w związku z ochroną danych osobowych.

Słowa kluczowe: ochrona danych osobowych, biblioteki publiczne, bezpieczeństwo informacji

Bardzo rzadko zdarza się, że jestem czymś zaskakiwana podczas szkoleń, jednak bibliotekarze z powiatu łęczyńskiego sprawili jakiś czas temu, że mówiąc kolokwialnie „szczęka mi opadła”. Spotykaliśmy się po raz drugi, po ponad rocznej przerwie w celu usystematyzowania wiedzy z poprzedniego szkolenia. Uczestnicy prawie bezbłędnie odpowiedzieli na pytania kontrolne, mające na celu sprawdzenie, co zapamiętali z ostatniego spotkania, a potem przeszliśmy do sprawdzania ich dokumentacji przetwarzania danych osobowych. Ich polityki bezpieczeństwa były przygotowane samodzielnie i doskonale. Moja rola ograniczyła się do porad, co można jeszcze dodać, jak pewne rzeczy ująć w lepszy sposób, jednakże nie byłam mentorem, a jedynie uprzejmym doradcą. Rozpierała mnie duma, że nastąpił taki postęp oraz, że wykazano aż takie zaangażowanie.

II. 1. Szkolenie z ochrony danych osobowych.
Gminna Biblioteka Publiczna w Krościenku Wyżnym.

Na pierwszym spotkaniu omawialiśmy absolutne podstawy. Bardzo często jest tak, że jestem zapraszana do bibliotek, żeby opowiedzieć „o co właściwie chodzi w tej ochronie danych osobowych" i „jak to zrobić, żeby się nie narobić". Najczęściej pierwsze szkolenie wiąże się z dość dużym stresem, bo uczestnicy dowiadują się, że nie dopełnili wielu ustawowych obowiązków i czeka ich dużo pracy. Tak też było w powiecie łęczyńskim. Po pierwszym spotkaniu wiedziałam, że czeka ich ogromna praca. Po drugim – stwierdziłam, że wykonano ją z nawiązką. Zresztą świadczyły o tym nie tylko dobrze zrobione polityki bezpieczeństwa oraz instrukcje zarządzania systemami informatycznymi, ale także to, że byli to jedyni klienci kupujący MAK-a+, którzy przed podpisaniem umowy zapytali o kwestię powierzenia przetwarzania danych osobowych.

Powierzenie danych na piśmie jest ustawowym obowiązkiem biblioteki (art. 31. *Ustawy o ochronie danych osobowych*, dalej UODO) zawsze wtedy, gdy zleca ona innemu podmiotowi czynności, które mogłaby wykonać samodzielnie, np. hosting danych, naprawa komputera/programu, tworzenie kopii zapasowych. Praktyka jednak pokazuje, że większość bibliotek nie wie nic na temat powierzenia przetwarzania danych osobowych i trzeba je przekonywać lub zmuszać, żeby podpisały umowę powierzenia (w przypadku MAK+ zapisy powierzenia są wplecione w umowę licencyjną, więc zawsze pozostaje argument, że nie można tego wykreślić). Brak umowy powierzenia między biblioteką a usługodawcą, stanowi wykroczenie z art. 51. i 52. UODO podlegające karze grzywny, ograniczenia lub pozbawienia wolności do 2 lat. Mówiąc krótko, brak umowy powierzenia oznacza, że dane zostały udostępnione nielegalnie – nawet jeżeli między biblioteką a usługodawcą została zawarta umowa na świadczenie usługi.

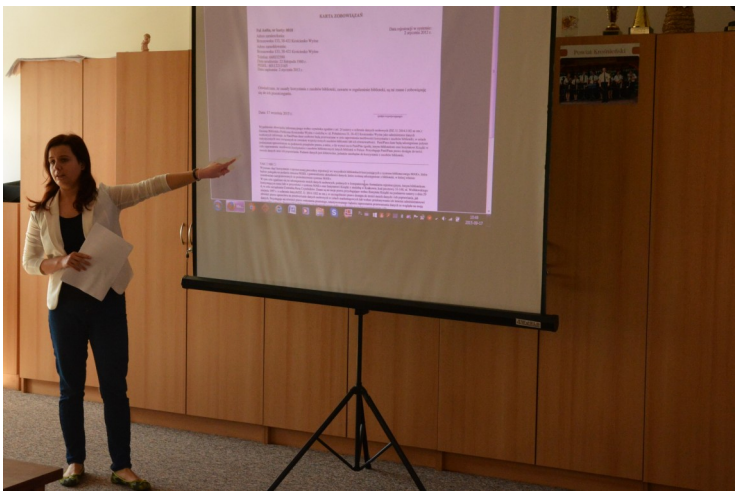
Z mojego doświadczenia w kontaktach z bibliotekami wynika, że większość z nich ma zgłoszony zbiór danych czytelników do Generalnego Inspektora Ochrony Danych Osobowych (GIODO), czyli prawidłowo wypełnia obowiązek wynikający z art. 40. UODO (zgłoszeniu nie podlegają tylko zbiory czytelników przetwarzane bez użycia systemu bibliotecznego). Inną sprawą jest, że często okazuje się, że zgłoszenia dokonał w imieniu biblioteki organizator i dyrektor żyje w nieświadomości tego faktu.

Czasami podczas szkoleń wyszukuję w jawnym rejestrze GIODO[1] (https://egiodo.giodo.gov.pl/personal_data_register.dhtml) biblioteki moich uczestników i widzę ogromne zdziwienie, że ich jednostka w tym rejestrze figuruje. Co więcej, nie wystarczy zgłosić zbiór, należy go jeszcze **aktualizować.** Typowe sytuacje, które pociągają za sobą obowiązek aktualizacji zbioru w rejestrze to: zmiana nazwy instytucji, w tym nadania patrona, zmiana adresu, powierzenie danych osobowych, zmiana zakresu przetwarzanych danych oraz rozpoczęcie przetwarzania danych czytelników w systemie bibliotecznym (do końca 2014 r. zgłoszeniu podlegały także zbiory czytelników przetwarzane tylko i wyłączenie w formie papierowej, od 2015 są zwolnione z tego obowiązku). Przeglądając rejestry zbiorów bibliotecznych, zauważyłam też, że bardzo często wśród informacji o czytelniku zaznaczono **zawód**, zamiast **kategorii społecznej**, myląc informację przesyłaną do GUS dotyczącą kategorii społecznej z zawodem wyuczonym czytelnika.

[1] Wszystkie odesłania do stron internetowych przedstawiają wersję aktualną w dn. 20.01.2016 r.

Po zmianie przepisów ustawy o ewidencji ludności i dowodach osobistych pojawił się dylemat, dotyczący braku adresu czytelnika w dowodzie osobistym. Należy wskazać, że większość bibliotek, po pierwszym wahaniu, podjęła decyzję o tym, żeby przyjmować ustne oświadczenie o miejscu zamieszkania czytelnika, które potwierdza się poprzez złożenie podpisu na karcie zobowiązania. Oceniam to rozwiązanie jako prawidłowe. Instytucje publiczne powinny wychodzić naprzeciw potrzebom obywateli, czyli nie wymagać od nich dodatkowych zaświadczeń o miejscu zamieszkania. Poza tym należy zauważyć, że do skutecznego odzyskania materiałów bibliotecznych lub ich równowartości jest niezbędny przede wszystkim numer ewidencyjny PESEL. Większość bibliotek wymaga go bezwzględnie, odmawiając wydania materiałów bibliotecznych poza obszar placówki bez jego podania (dopuszczają udostępnienie na miejscu). W mojej ocenie jest to bardzo prawidłowa postawa. Wiem, że w praktyce czytelnicy często nie chcą udostępniać numeru PESEL (uważają, że bibliotece nie jest on potrzebny i że jest to przekroczenie uprawnień/wymysł bibliotekarza). Bibliotekarze najczęściej informują wtedy, że *ich system biblioteczny wymaga numeru PESEL i bez niego niemożliwe jest zarejestrowanie w bibliotece*. Nawet jeżeli system wymaga, nie jest to powód prawdziwy. Obowiązek podawania numeru PESEL przez czytelnika jest umotywowany przepisami *Ustawy o bibliotekach*, która narzuca na biblioteki obowiązek ochrony materiałów bibliotecznych, gdyż stanowią szczególnie chronione dobro kultury. Z ustawy wynika, że biblioteka musi zrobić wszystko, co w jej mocy, aby być w stanie odzyskać udostępnione materiały.

Niektóre biblioteki od samego początku wymagały numeru PESEL, inne dopiero od niedawna wprowadziły taką regułę. Najczęściej okazuje się, że w tych bibliotekach, przed wymaganiem numeru PESEL, proszono o podanie imienia ojca, co stanowiło dodatkowy identyfikator. Warto rozważyć, czy w dalszym ciągu istnieje uzasadnienie do wymagania (lub przechowywania w bazie) informacji o imieniu ojca czytelnika. Czy przetwarzanie tych danych jest adekwatne do celu przetwarzania? Ustawa o ochronie danych osobowych wyraźnie wskazuje na konieczność weryfikacji zakresu zbieranych danych pod kątem ich przydatności – czy na pewno są one niezbędne do zrealizowania celu, dla którego zostały zebrane. Jeżeli nie, należy je bezwzględnie usunąć.



II. 2. Szkolenie z ochrony danych osobowych.
Gminna Biblioteka Publiczna w Krościenku Wyżnym.

Niektórzy czytelnicy wysyłają skargi do GIODO na obowiązek podawania numeru PESEL w bibliotece, czego konsekwencją jest wysłanie przez Biuro GIODO pisma do dyrektora biblioteki z prośbą o uzasadnienie adekwatności wymagania tej informacji. Pismo od Generalnego Inspektora nie oznacza, że bibliotekarze zrobili coś źle, a jedynie, że musi on wyjaśnić przyczynę skargi oraz ustalić, czy jest uzasadniona. Jeżeli zgodzi się z argumentami biblioteki na adekwatność wymagania numeru PESEL (a jego wymaganie jest niepodważalne w związku z koniecznością możliwości odzyskania zbiorów), przekaże tę informację osobie wnoszącej skargę.

W mojej ocenie, dużym zaniedbaniem jest brak niszczarek w bibliotekach, w szczególności w filiach bibliotecznych. Darcie kartek nie gwarantuje ich skutecznego zniszczenia, a komisyjne przekazywanie ich do biblioteki głównej w celu zniszczenia jest dość pracochłonne i problematyczne. Przepisy nie określają standardu niszczarki, która powinna być zakupiona do biblioteki, wystarczyłoby, aby była to malutka niszczarka, zakładana na kosz na śmieci, której koszt nie przekracza 40 zł. Częstą praktyką jest też zabieranie przez jednego z pracowników dokumentów do domu, w celu spalenia w piecu. Chciałabym zwrócić uwagę, że o ile sama metoda jest skuteczna, to procedura powinna być taka, żeby fakt zniszczenia nie ulegał wątpliwości, żeby nikt nie mógł zarzucić, że te dokumenty nie zostały faktycznie zniszczone. Wystarczyłoby powołać komisję (przynajmniej dwie osoby), która dokonałaby komisyjnego spalenia dokumentów i spisała z tej czynności protokół.

Podsumowując, z ochroną danych w bibliotekach jest na pewno coraz lepiej. Jestem przekonana o tym, że bibliotekarze i dyrektorzy bibliotek dokładają starań, aby skutecznie chronić dane, zwłaszcza czytelników. Często zapominają o tym, że kwestie organizacyjne dotyczące ochrony danych powinny zostać spisane i przedstawione wszystkim osobom dopuszczonym do pracy z danymi (lub w pomieszczeniach z danymi), jednak w porównaniu do stanu sprzed kilku lat jest już coraz mniej bibliotek, w których nie ma w ogóle polityki bezpieczeństwa czy instrukcji zarządzania systemami informatycznymi.

Inną bolączką jest brak osoby administrującej systemy informatyczne i dbającej o bezpieczeństwo sieci. Wiele bibliotek gminnych w ogóle nie ma informatyka i borykają się z ogromnym problemem skutecznego zabezpieczenia danych elektronicznych. Jest to jedna z ważniejszych kwestii do rozwiązania, zwłaszcza w tych bibliotekach, które udostępniają komputery czytelnikom. Biblioteka staje się bardzo atrakcyjnym miejscem do popełnienia cyberprzestępstwa, dlatego konieczna jest właściwa ochrona i monitoring sieci. Administrator systemów informatycznych dba także o bezpieczeństwo komputerów bibliotekarzy, chociażby przez ograniczenie ich uprawnień (tylko on powinien móc instalować oprogramowanie), dba o aktualne licencje na oprogramowanie antywirusowe, czy systemowe. Wymusza też odpowiednią politykę haseł i obowiązek blokowania komputera (kombinacja klawiszy Windows + L), gdy się od niego odchodzi. Są to zasady bezpieczeństwa określone w przepisach wykonawczych do ustawy o ochronie danych osobowych, a nie wymysł informatyka. W przepisach jest wskazane wprost, że każdy użytkownik (bibliotekarz) musi logować się do systemu (Windowsa, systemu bibliotecznego, Płatnika itd.) na swój indywidualny identyfikator i hasło, które nie dość, że musi mieć odpowiednią znakową złożoność, to musi być zmieniane co 30 dni. Mówiąc krótko, administrator systemów informatycznych ma niewdzięczną rolę, ale jego praca jest bardzo ważna dla całej jednostki.

Warto mu zaufać i wymagać od pracowników, aby przestrzegali narzuconych przez niego reguł.

Bardzo pozytywnie oceniam to, że biblioteki zaczynają nie tylko dbać o bezpieczeństwo danych, ale przeprowadzają też odpowiednie działania prewencyjne w postaci szkoleń dla pracowników oraz audytów bezpieczeństwa. Są to czynności, które może samodzielnie wykonać dyrektor lub wyznaczona przez niego osoba. Nie ma obowiązku korzystania z certyfikowanych firm szkoleniowo-audytowych. Przepisy określają, że dyrektor powinien zapewnić w ramach swoich możliwości zapoznanie pracowników z obowiązującymi przepisami oraz regulacjami wewnętrznymi w bibliotece. To on decyduje, w jaki sposób tego dokona. Przeprowadzanie okresowych kontroli jest najlepszym sprawdzeniem kondycji bezpieczeństwa informacji w zarządzanej jednostce. Pozwala sprawdzić, na ile określone zasady są realizowane w praktyce. Powtarzane regularnie pozwalają wyeliminować wiele problemów.

Świadomość konieczności wielu zmian jest duża, więc myślę, że różne niedociągnięcia będą z czasem coraz mniejsze, a ja na swoich szkoleniach będę mogła coraz więcej nauczyć się od uczestników. To są moi najlepsi i najbardziej wymagający uczniowie oraz bardzo zdolni nauczyciele. Współpraca z nimi daje bardzo dużo satysfakcji.

Sylwia Czub-Kiełczewska: Specjalista ds. ochrony danych osobowych i informacji niejawnych. Koordynator ochrony danych osobowych w Instytucie Książki. Ekspert w dziedzinie ochrony danych w bibliotekach. Prowadzi blog poświęcony zagadnieniom ochrony danych osobowych w praktyce: sylwiaczub.pl.

Czub-Kiełczewska, S. Przepisy o ochronie danych osobowych – jak biblioteki sobie z tym radzą? *Biuletyn EBIB* [on-line] 2015, nr 1 (163), *Prywatność w bibliotece.* [Dostęp 25.02.2016]. Dostępny w: http://open.e-bib.pl/ojs/index.php/ebib/article/view/404. ISSN 1507-7187.