Fundacja Rozwoju Bankowości Spółdzielczej
Grupa BPS

Oferta outsourcingu obowiązków ABI dla Banków Spółdzielczych

KONTAKT W SPRAWIE OFERTY:

Piotr Uliński
Koordynator Szkoleń
tel. kom.: 797 308 502
e-mail: piotr.ulinski@frbs.org.pl

Fundacja Rozwoju Bankowości Spółdzielczej
Grupa BPS

Szanowni Państwo,

Fundacja Rozwoju Bankowości Spółdzielczej przygotowała dla Państwa ofertę profesjonalnego outsourcingu obowiązków Administratora Bezpieczeństwa Informacji.

Outsourcing ABI polega **na przejęciu obowiązków wynikających z przepisów ustawy o ochronie danych osobowych**. Ze względu na skalę przetwarzania danych, odpowiedzialność prawną za ich przetwarzanie i ryzyko reputacyjne GIODO rekomenduje powołanie w bankach Administrator Bezpieczeństwa Informacji (ABI). ABI to osoba wyznaczona przez administratora danych do pełnienia funkcji związanych z szeroką pojętą ochroną danych osobowych. Posiadanie profesjonalnego ABI to gwarancja bezpieczeństwa przetwarzania danych osobowych.

Założenia oferty, jej zakres, możliwości wyboru sposobu współpracy oraz sylwetkę eksperta przedstawiamy w dalszej części.

Z poważaniem,

Krzysztof Story
Prezes Zarządu

Fundacja Rozwoju Bankowości Spółdzielczej
30-556 Kraków, ul. Wodna 2
tel./fax: 12 26 50 912, e-mail:FRBS.Krakow@bankbps.pl

Fundacja Rozwoju Bankowości Spółdzielczej
Grupa BPS

Dlaczego warto powołać zewnętrznego administratora bezpieczeństwa informacji?

Z dniem 1 stycznia 2015 roku weszły w życie ważne zmiany w ustawie o ochronie danych osobowych dotyczące m.in. instytucji administratora bezpieczeństwa informacji (ABI). Przed nowelizacją administrator danych miał obowiązek wyznaczenia ABI, chyba, że był osobą fizyczną prowadzącą działalność gospodarczą – wtedy mógł sam wykonywać jego czynności. Obecnie obowiązujące przepisy dają administratorom danych prawo wyboru – sami decydują, czy chcą powołać ABI czy nie. Czy zatem posiadanie ABI leży w interesie administratora danych?

Zmieniona ustawa nałożyła na administratorów bezpieczeństwa informacji szereg nowych obowiązków. Obecnie do zadań ABI należy:

1. zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
   - ✓ sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,
   - ✓ nadzorowanie opracowania i aktualizowania polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym, oraz przestrzegania zasad w nich określonych,
   - ✓ zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych
2. prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych.

Należy podkreślić, że w przypadku, gdy ABI nie zostanie powołany, wyżej wymienione obowiązki spoczywać będą na administratorze danych. Dlatego też posiadanie wykwalifikowanego ABI może okazać się bardzo pomocne.

Warto zdecydować się na outsourcing wszystkich lub wybranych zadań i powołanie zewnętrznego ABI, ponieważ:

Wymagania względem ABI	Korzyści z outsourcingu
Pełny zakres obowiązków z ustawy (art. 36b)	Na bankach, które nie powołają ABI ciążą wszystkie obowiązki ustawowe (art. 36b ustawy) i są zobowiązane do wywiązywania się z nich. **Powierzenie ich osobie, która ma wieloletnie doświadczenie w zarządzaniu ochroną danych w bankach to najprostszy sposób na właściwe zabezpieczenie interesów banku.**
Wymóg odpowiedniej wiedzy (art. 36a ust. 5 pkt 2)	Od 1 stycznie 2015 roku ustawa wymaga, aby ABI posiadał odpowiednią wiedzę w zakresie ochrony danych osobowych (art. 36a ust. 5 pkt 2 ustawy). **Nasz ekspert dysponuje unikalnym doświadczeniem zawodowym i wykształceniem w dziedzinie ochrony danych osobowych w bankach, które wyróżnia go na rynku.** Od wielu lat współpracuje z kilkudziesięcioma Bankami Spółdzielczymi Zrzeszenia BPS oraz z Bankiem Polskiej Spółdzielczości i Fundacją Rozwoju Bankowości Spółdzielczej. Był

	administratorem bezpieczeństwa informacji w wielu bankach, również zagranicą, od 1998 r., a więc od wejścia w życie ustawy o ochronie danych osobowych.
Zakaz powoływania Wiceprezesa Zarządu na ABI (art. 36a ust. 8 ustawy)	Powierzenie funkcji ABI Wiceprezesowi Zarządu zostało wykluczone przez GIODO, a zgłoszenie tej osoby jako ABI zostanie przez GIODO odrzucone. **Outsourcing to najprostszy sposób zapewnienia organizacyjnej odrębności ABI w ramach banku.**
Zakaz kolizji obowiązków ABI z innymi zadaniami (art. 36a ust. 4 ustawy)	Najczęściej na stanowisko ABI powoływani są pracownicy już zatrudnieni w banku co skutkuje nałożeniem na taką osobę dodatkowych obowiązków. Zwykle obowiązki dotyczące ochrony danych osobowych są tylko drobną częścią zakresu zadań wyznaczonego pracownika, mimo że są wymagające i czasochłonne. Powoduje to częste naruszenia ustawy. **Outsourcing rozwiązuje również problem wynikający z tego, że zgodnie z ustawą bank może powierzyć ABI wykonywanie innych obowiązków, tylko jeżeli nie naruszy to prawidłowego wykonywania ustawowych zadań ABI.**
Wymóg pozycji w strukturze Banku i zapewnienia środków (art. 36a ust. 7 i 8)	Ustawa wymaga, aby ABI podlegał bezpośrednio kierownikowi jednostki organizacyjnej. (art. 36a ust. 7). **Z jednej strony ustawa nakłada obowiązek wysokiej pozycji ABI w strukturze Banku, ale z drugiej GIODO zakazuje powierzenia stanowiska ABI Wiceprezesowi Zarządu Banku Spółdzielczego.** Ustawa wymaga także, aby Bank zapewnił ABI środki niezbędne do niezależnego wykonywania zadań przez ABI (art. 36a ust. 7 i 8). Outsourcing funkcji ABI rozwiązuje te problemy.
Obowiązek poddawania ochrony danych okresowym audytom. Możliwość wykorzystania sprawozdania w raporcie Zarządu dla RN	Każdy bank ma obowiązek poddawania ochrony danych okresowym audytom w zakresie określonym w rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. (art. 36a ust. 2 pkt 1 lit. a ustawy). **Zlecając pełny outsourcing zewnętrznemu ABI audyt i sprawozdanie z niego będą wchodzić w zakres obowiązków ABI.** Sprawozdanie może być ponadto wprost wykorzystane w ramach okresowego obowiązkowego raportowania zgodności przez Zarząd Radzie Nadzorczej.
Obowiązek rejestracji zbiorów	Powołanie ABI ułatwia proces obowiązkowej rejestracji zbiorów danych i aktualizacji zgłoszeń rejestracyjnych.
ABI w banku	**Obecnie powołanie ABI w bankach jest zalecane przez GIODO, a zgodnie z założeniami nadchodzącej reformy w przyszłości powołanie ABI w bankach ponownie będzie konieczne.**

Outsourcing nie wymaga etatu i zasadniczo zmniejsza koszty zapewnienia zgodności przy zachowaniu wysokiej jakości

Zakres oferty:

Aby zapewnić Bankom elastyczność i wybór oferujemy różne opcje współpracy wraz ze szczegółowymi opisami poszczególnych działań.

Wybór tych opcji zależy w pełni od Banku. Możliwe jest również indywidulane kształtowanie zakresu współpracy wykraczającego poza te opcje.

Opcja 1

Audyt wymagany przez prawo

(kompleksowy audyt otwarcia)

Zgodność przetwarzania danych osobowych z przepisami musi być okresowo weryfikowana.

Zakres wewnętrznego audytu określa rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. poz. 745).

Opis audytu

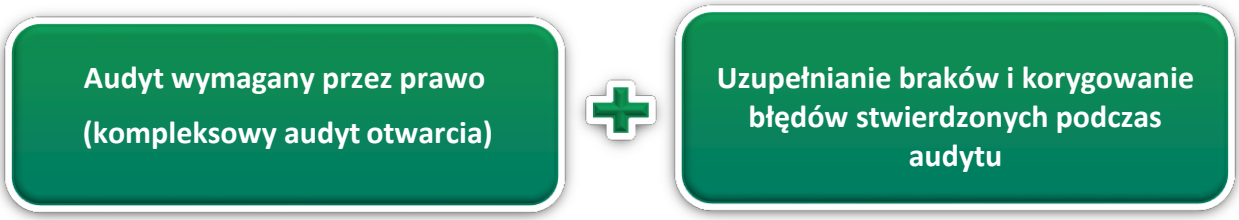
Audyt obejmuje analizę dokumentów oraz wizytę w Banku i rozmowy z pracownikami.
Raport jest przedstawiany Zarządowi Banku Spółdzielczego.

Zakres raportu w Opcji 1 obejmie określenie:

- ✓ obowiązków prawnych w ramach kategorii określonych przez MAC
- ✓ stwierdzonego stanu faktycznego
- ✓ rekomendacji
- ✓ gradacji rekomendacji wg zasady risk-based approach, która obejmuje:
  - obserwacje (drobna uwagi, sugestie), które nie wpływają zasadniczo na ogólną ocenę zgodności z prawem
  - średnie niezgodności wymagające korekty
  - znaczne naruszenia, których skutkiem jest niezgodność działania z prawe

Należy przeprowadzić co najmniej jeden planowy audyt ochrony danych rocznie, a przypadku podejrzenia naruszenia również audyt doraźny.

Opcja 2

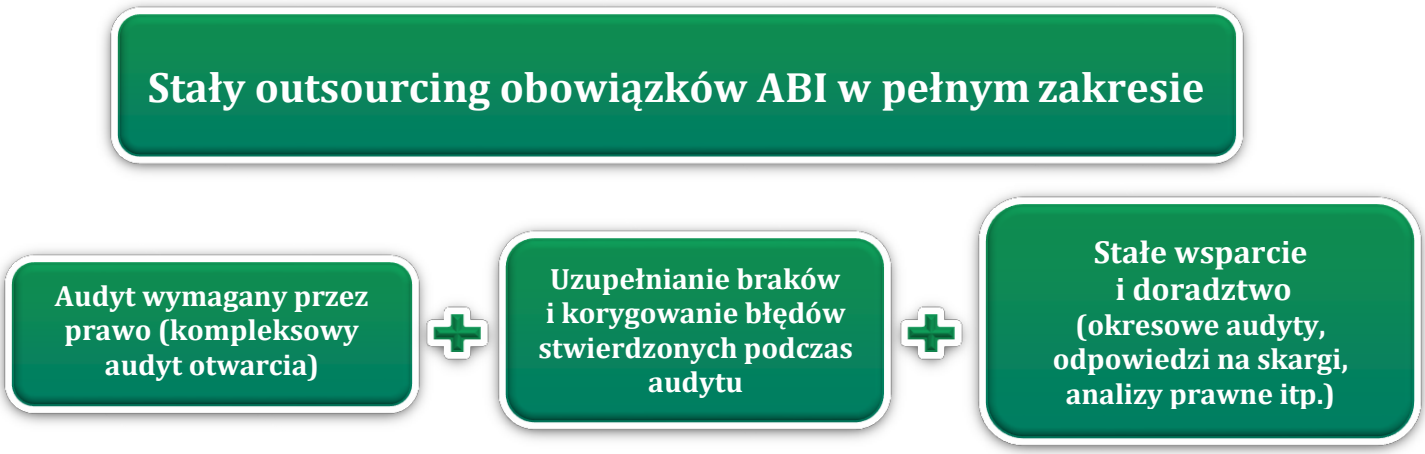


Uzupełnianie braków i korygowanie błędów stwierdzonych podczas audytu obejmuje:

- ✓ opracowanie lub korekta dokumentacji wymaganej przez ustawę oraz rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. (polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych),
- ✓ dodatkowe instrukcje składające się na system ochrony danych w banku, np. instrukcja postępowania w przypadku naruszenia ochrony i inne,
- ✓ opracowanie lub korekta klauzul zgody i klauzul informacyjnych,
- ✓ upoważnienia do przetwarzania danych osobowych dla pracowników, ewidencja osób upoważnionych, zobowiązania do zachowania poufności,
- ✓ zapewnienie zgodności umowom outsourcingu,
- ✓ rejestracja zbiorów danych lub weryfikacja rejestrów.

Fundacja Rozwoju Bankowości Spółdzielczej
Grupa BPS

Opcja 3



Stały outsourcing obowiązków administratora bezpieczeństwa informacji (ABI) w ramach abonamentu obejmuje zakres obowiązków:

1. **Opcje 1 i opcję 2 tj.:**
   - ✓ audyt wymagany przez prawo (kompleksowy audyt otwarcia)
   - ✓ uzupełnianie braków i korygowanie błędów stwierdzonych podczas audytu otwarcia

2. **oraz stałe wsparcie i doradztwo obejmujące:**
   - ✓ śledzenie zmian w przepisach o ochronie danych,
   - ✓ w razie potrzeby aktualizację dokumentacji i procedur,
   - ✓ obowiązkowe coroczne audyty ochrony danych, sprawozdania z audytu dla Zarządu banku,
   - ✓ prowadzenie obowiązkowego rejestru zbiorów danych osobowych,
   - ✓ help desk – pomoc (e-mailowo lub telefoniczne) w razie wątpliwości lub problemów dotyczących ochrony danych osobowych i tajemnicy bankowej (2 x miesięcznie z wyznaczonym przedstawicielem banku),
   - ✓ odpowiedzi na pisemne skargi klientów dotyczące naruszeń ustawy o ochronie danych osobowych,,
   - ✓ reprezentowanie banku przed GIODO (w tym korespondencja), KNF i audytorami BPS w zakresie ustawy o ochronie danych osobowych i tajemnicy bankowej,
   - ✓ opiniowanie umów outsourcingu w zakresie ochrony danych osobowych i tajemnicy bankowej,
   - ✓ raz na rok wizytę w banku.

Opiekę nad ochroną danych w Państwa Banku będzie sprawował ekspert

dr MARIUSZ KRZYSZTOFEK

Ustawa wymaga, aby administrator bezpieczeństwa informacji posiadał odpowiednią wiedzę w zakresie ochrony danych osobowych. Nasz ekspert dysponuje unikalnym doświadczeniem zawodowym i wykształceniem w dziedzinie ochrony danych osobowych w bankach, które wyróżnia go na rynku.

- ✓ od wielu współpracuje z kilkudziesięcioma Bankami Spółdzielczymi Zrzeszenia BPS oraz z Bankiem Polskiej Spółdzielczości i Fundacją Rozwoju Bankowości Spółdzielczej,

- ✓ był administratorem bezpieczeństwa informacji w wielu instytucjach od 1998 r., a więc od wejścia w życie ustawy o ochronie danych osobowych. M.in. w Banku Polskiej Spółdzielczości, BGŻ BNP Paribas, a także zagranicą jako Data Protection Coordination Officer w Brukseli oraz Head of Compliance & Regulatory dla polskiego oddziału jednej z największych międzynarodowych grup finansowych,
- ✓ wśród podmiotów, z którymi współpracował, znajdują przede wszystkim banki, w tym liczne Banki Spółdzielcze, oraz inne instytucje finansowe. Ponadto firmy z wielu innych sektorów, polskie i zagraniczne: informatyczne, paliwowe, pocztowe, a także uczelnie wyższe oraz organy państwowe: sądy, Ministerstwo Sprawiedliwości, czy Komisja Nadzoru Finansowego. Łącznie to ponad 100 instytucji, wiele kilkakrotnie,
- ✓ jest autorem 3 książek na temat ochrony danych osobowych, najnowsza z nich to „Tajemnice zawodowe i ochrona danych osobowych w instytucjach finansowych", Wolters Kluwer SA, 2015.
- ✓ W 2016 r. zagranicą ukaże się jego kolejna książka (na temat unijnej reformy ochrony danych) - "The protection of personal data in the European Union", w języku angielskim, przeznaczona na rynki europejskie,
- ✓ był wielokrotnie prelegentem na konferencjach na temat ochrony danych, w Polsce i zagranicą, również wraz z GIODO,
- ✓ od wielu lat prowadzi szkolenia i konsultacje z ochrony danych; za działalność szkoleniową na rzecz banków został odznaczony przez Związek Banków Polskich Odznaką Honorową, ponadto wyróżniony jako „Wzorowy Trener WIB roku 2011, 2012, 2013, 2014" oraz „Trener XX-lecia",
- ✓ był wielokrotnie ekspertem w programach telewizyjnych poświęconych ochronie danych osobowych, m.in. w TVN24, Polsat News, TVN CNBC Biznes, TVP Info,
- ✓ wystąpił przed sejmową Komisją Sprawiedliwości i Praw Człowieka w sprawie projektu nowelizacji ustawy ochronie danych osobowych oraz jest autorem projektu zmiany przepisów o tajemnicy bankowej przyjętej przez Ministra Sprawiedliwości.

ZAPRASZAMY DO WSPÓŁPRACY

KONTAKT W SPRAWIE OFERTY:

Wszelkich dodatkowych informacji udzieli Państwu:

Piotr Uliński
Koordynator szkoleń

tel. kom.: 797 308 502
e-mail: piotr.ulinski@frbs.org.pl