Kancelaria Prezesa
Rady Ministrów

Marek Kuchciński

DNK.WK.1741.6.2022.JG
Warszawa, 28 grudnia 2022 r.

Pan
Bartłomiej Chmielowiec
Rzecznik Praw Pacjenta

WYSTĄPIENIE POKONTROLNE

Przedstawiam Panu Ministrowi Wystąpienie pokontrolne (dalej: Wystąpienie) z kontroli przeprowadzonej przez Kancelarię Prezesa Rady Ministrów w Biurze Rzecznika Praw Pacjenta (dalej: BRPP, Biuro, Jednostka) w zakresie *wybranych aspektów zarządzania bezpieczeństwem informacji w latach 2021-2022*[1].

Podstawa prawna:
Art. 25 ust. 1 pkt 3 lit. b i 25a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[2] (dalej: *ustawa o informatyzacji*) oraz art. 46 i 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[3] (dalej: *ustawa o kontroli*)

OCENA KONTROLOWANEGO OBSZARU

Biuro nie zapewniło odpowiedniego poziomu bezpieczeństwa przetwarzanych informacji wykorzystywanych do realizacji zadań publicznych. W zbadanych obszarach stwierdzono liczne braki i nieprawidłowości, których usunięcie wymaga podjęcia niezwłocznych działań naprawczych w celu zapewnienia bezpieczeństwa informacji (dalej: BI). BRPP nie opracowało kompleksowego i spójnego systemu zarządzania bezpieczeństwem informacji (dalej: SZBI) gwarantującego poufność, dostępność i integralność przetwarzanych danych wykorzystywanych do realizacji zadań publicznych.

Pomimo upływu ponad 10 lat od wejścia w życie Rozporządzenia KRI[4] i ponad 13 lat funkcjonowania BRPP, w których obowiązywała *ustawa o informatyzacji*[5], Biuro nie dysponuje najważniejszym i podstawowym dokumentem SZBI, jakim jest Polityka Bezpieczeństwa Informacji (dalej: PBI). Wewnętrzne regulacje dotyczyły wyłącznie ochrony danych osobowych.

Badaniem objęto następujące obszary zarządzania BI:

- nadzór Kierownictwa BRPP nad SZBI;
- okresowe analizy ryzyka utraty integralności, dostępności lub poufności informacji;
- audyt wewnętrzny w zakresie BI;
- szkolenia osób zaangażowanych w proces przetwarzania informacji;
- bezpieczna praca przy mobilnym przetwarzaniu danych i pracy na odległość;
- wykonywanie kopii zapasowych;

[1] Rzecznik Praw Pacjenta nie złożył zastrzeżeń do projektu wystąpienia pokontrolnego.
[2] Dz. U. z 2021 r., poz. 2070, t. j. ze zm. W okresie objętym kontrolą obowiązywał również t. j. opublikowany w Dz. U. z 2020 r. poz. 346 oraz z 2021 r. poz. 670.
[3] Dz. U. z 2020 r., poz. 224 t. j.
[4] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247, t. j.). Wejście w życie 31 maja 2012 r.
[5] BRPP utworzono w 2009 r. *Ustawa o informatyzacji* weszła w życie 21 lipca 2005 r.

- rejestr zasobów teleinformatycznych (baza konfiguracji CMDB).

Proces opracowania SZBI należy rozpocząć od całościowego przeglądu stanu BI, z wykorzystaniem informacji przekazanych przez Szefa KPRM i przeprowadzenia rzetelnej analizy ryzyka wszystkich aktywów Jednostki na podstawie przyjętych zasad. Do zarządzania tym systemem niezbędne jest określenie szczegółowej dokumentacji, w tym PBI oraz wprowadzenie narzędzi nadzorczych dostarczających Kierownictwu BRPP pełnych informacji nt. poszczególnych etapów jego wdrażania. Pilne wdrożenie rekomendacji audytu przyczyni się do usprawnienia tego procesu w organizacji i wsparcia Rzecznika Praw Pacjenta w zarządzaniu obszarem BI.

Istotnym jest, że Biuro nie dysponuje specjalistami w zakresie BI. Jednostka podejmowała próby pozyskania środków finansowych na wprowadzenie SZBI przez podmiot zewnętrzny, ale były one nieskuteczne. Z uwagi na realizowane zadania w zakresie ochrony praw pacjentów, BRPP powinno poddać analizie i ocenić ryzyko powierzenia opracowania SZBI zewnętrznemu usługodawcy.

> BRPP użytkuje jeden system teleinformatyczny, tj. EZD PUW (system do elektronicznego zarządzania dokumentacją autorstwa Podlaskiego Urzędu Wojewódzkiego w Białymstoku). System ten służy do elektronicznego zarządzania dokumentacją. Wdrażany jest w administracji rządowej jako jednolity system, rozwijany na zasadach niekomercyjnych, będący narzędziem wymiany informacji oraz usprawnienia funkcjonowania urzędów.

Elementy Systemu Zarządzania Bezpieczeństwem Informacji

- **[PBI]** Pomimo upływu ponad 10 lat od wejścia w życie Rozporządzenia KRI i ponad 13 lat funkcjonowania BRPP, w których obowiązywała *ustawa o informatyzacji*, Biuro nie posiadało kompleksowego SZBI. W szczególności dotyczy to braku opracowania całościowej dokumentacji, która jest warunkiem skutecznego zarządzania BI. Jednostka nie dysponowała najważniejszym i podstawowym dokumentem SZBI, jakim jest PBI, ponieważ obowiązująca regulacja dotyczyła wyłącznie ochrony danych osobowych.
- **[Nadzór Kierownictwa i analiza stanu BI]** Kierownictwo BRPP nie posiadało skutecznych narzędzi zarządczych zapewniających nadzór nad BI. Nie dokonano analizy stanu BI, co byłoby podstawą do ustanowienia adekwatnego do potrzeb Biura SZBI. Natomiast brak dokumentowania spotkań Kierownictwa Biura z dyrektorami departamentów uniemożliwiał skuteczne monitorowanie i ocenę podjętych w ich wyniku decyzji i działań.
- **[Role i odpowiedzialność]** Nie ustalono ról i odpowiedzialności głównych osób zaangażowanych w BI, za wyjątkiem Dyrektora Departamentu Organizacyjno-Administracyjnego (dalej: DOA) i zdefiniowania ról administratora systemów informatycznych (dalej: ASI) i jego zastępcy oraz roli administratora właściwego. W konsekwencji nie było możliwe przypisanie konkretnym osobom pełnej odpowiedzialności za rozwój i wdrażanie BI oraz określenie osób, które wspierały Kierownictwo w określaniu adekwatnych zabezpieczeń.
- **[Analiza ryzyka]** Nie przeprowadzono analizy ryzyka utraty integralności, dostępności i poufności informacji, czym naruszono obowiązek określony w § 20 ust. 2 pkt 3 Rozporządzenia KRI. Bez analizy ryzyka nie jest możliwe skuteczne zaprojektowanie zabezpieczeń – ich rodzaju i poziomu.
- **[Audyt]** W Biurze zrealizowano audyt BI, ale nie objęto nim wszystkich obszarów SZBI. Tym samym nie zapewniono pełnej oceny funkcjonujących rozwiązań. Negatywnie należy ocenić niewdrożenie rekomendacji audytu ze względu na ich istotność dla tego obszaru.

- **[Baza CMDB]** Nie utworzono bazy konfiguracji CMDB, tym samym nie spełniono wymogów określonych w § 20 ust. 2 pkt 2 Rozporządzenia KRI, mimo że Biuro posiada narzędzie (IT Manager) do ewidencjonowania zasobów informatycznych innych niż komputery, zapewniające możliwość tworzenia relacji pomiędzy umieszczonymi w bazie zasobami[6]. Niemożliwe było zatem efektywne zarządzanie infrastrukturą informatyczną, czy też przeprowadzenie rzetelnej analizy ryzyka i przygotowanie planu postępowania z ryzykiem.
- **[Praca zdalna]** W regulacjach określono najistotniejsze kwestie związane z BI. Zastrzeżenia budzi brak wskazania opisu wymaganych zabezpieczeń w przypadkach dopuszczenia możliwości korzystania z domowej sieci Wi-Fi. Pozytywnie należy ocenić, że wszystkie urządzenia mobilne (95) w prawidłowy sposób zabezpieczano pod kątem uwierzytelniania użytkownika, bezpiecznego szyfrowania połączenia VPN oraz instalacji oprogramowania antywirusowego. Natomiast 15 z 95 (16%) najstarszych z urządzeń było narażonych na utratę danych, ponieważ nie objęto ich, tak jak 84% pozostałych urządzeń, systemem [redacted] zabezpieczającym aplikacje i dane oraz kontrolującym urządzenia przenośne. Nie zachowano rozliczalności działań pracowników pracujących zdalnie, ponieważ nie wdrożono narzędzi umożliwiających monitorowanie zdalnego dostępu do zasobów i systemów.
- **[Kopie zapasowe]** Prawidłowym działaniem było wykonywanie kopii zapasowych badanego systemu teleinformatycznego, tj. EZD PUW. Okres ich retencji był właściwy i wynosił 1 miesiąc. Jednakże niewłaściwym było to, że kopie testowano raz na kwartał oraz przechowywano je w tej samej lokalizacji, w którym uruchomiony był EZD PUW. Ponadto nie zaktualizowano i uzupełniono regulacji wewnętrznych o szczegółowe zasady związane z zakresem wykonywania kopii zapasowych, ich przechowywaniem w innym miejscu, częstotliwością przeprowadzania testów związanych z odtworzeniem kopii zapasowych.
- **[Szkolenia]** Wzmocnienia wymagają działania dot. zwiększania świadomości pracowników w zakresie BI. Szkolenie odbyło tylko 48 z 115 (42%)[7] pracowników, i nie przeszkolono żadnego z 40 stażystów, praktykantów i wolontariuszy. W BRPP nie funkcjonował wymóg złożenia przez użytkowników oświadczenia o zobowiązaniu się do przestrzegania zasad dot. ochrony i BI.

OCENY I USTALENIA SZCZEGÓŁOWE

I. Elementy Systemu Zarządzania Bezpieczeństwem Informacji

1. [PBI] Biuro nie opracowało i nie wdrożyło PBI, a wybrane jej elementy uregulowano w innych dokumentach. Stanowi to naruszenie § 20 ust. 1 Rozporządzenia KRI. Brak tak podstawowej regulacji może prowadzić do ryzyka utraty dostępności, integralności i poufności informacji, a w konsekwencji może istotnie wpływać na stabilność pracy Biura.

W BRPP nie wprowadzono PBI. Niektóre elementy dot. BI funkcjonowały w ramach innych dokumentów, tj.: *Polityki Ochrony Danych Osobowych*[8] oraz *Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w BRPP*[9] (dalej: *Instrukcja danych osobowych*).

Jak podano[10], Biuro w 2021 r. i 2022 r. nie dysponowało wystarczającym budżetem na wdrożenie SZBI poprzez usługę zewnętrzną, a pracownicy działu IT (tj. dwóch studentów) nie posiadali wystarczających kwalifikacji do realizacji tego zadania.

---

[6] https://www.it-man.pl/funkcjonalnosc/zarzadzanie-zasobami/, dostęp: 17.11.2022 r.
[7] Zatrudnionych na dzień 19 września 2022 r., którzy odbyli szkolenia w okresie objętym kontrolą.
[8] Stanowiącej zał. nr 1 do *zarządzenia nr 11/2022 Rzecznika Praw Pacjenta z dnia 19 maja 2022 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w BRPP oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w BRPP* (dalej: *zarządzenie*).
[9] Stanowiącą załącznik nr 2 do *zarządzenia*.
[10] Pismo z 13 września 2022 r., znak: RzPP-DOA-WOR.091.3.2022 oraz z 17 października 2022 r., znak: RzPP-DOA-WOR.091.3.2022

Do braku środków finansowych przyczyniła się pandemia COVID-19, a BRPP, oprócz jednorazowego wsparcia z rezerwy ogólnej na działanie Telefonicznej Informacji Pacjenta, nie otrzymało innych środków. Od 2020 r. Biuro podejmowało działania mające na celu otrzymanie dodatkowych funduszy na stworzenie kompleksowej dokumentacji SZBI. Zdaniem BRPP niedofinansowanie Biura przekładało się na zabezpieczanie w ostatnich latach wydatków dotyczących wzmocnienia obszarów objętych kontrolą[11]. Dopiero w projekcie ustawy budżetowej na 2023 r. przewidziano środki na 1 etat dla specjalisty w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji.

Jednostka zobowiązała się, że w planowanej kompleksowej dokumentacji SZBI ujmie wszelkie wytyczne, zalecenia i dobre praktyki w zakresie BI, w szczególności dot. podziału ról i odpowiedzialności, realizacji audytu, prowadzenia bazy konfiguracji CMDB, szkoleń.

Nie można zgodzić się z wyjaśnieniami Kontrolowanego. Po pierwsze, lata 2021-2022 to okres funkcjonowania w pandemii COVID-19 i narażenie na wysokie ryzyko utraty integralności, dostępności i poufności informacji przetwarzanych w Jednostce. Biuro już wtedy powinno dysponować ustanowioną i wdrożoną PBI, ponieważ BRPP powstało w 2009 r.[12], a regulacje dot. obszaru BI powinny być priorytetem. Po drugie, opracowanie PBI nie wymaga dodatkowych nakładów finansowych, szczególnie w przypadku małej jednostki, jaką jest BRPP. Ponadto niemożliwym jest budowanie SZBI bez uprzedniego wdrożenia PBI oraz przeprowadzenia analizy ryzyka.

2. [nadzór Kierownictwa] Kierownictwo BRPP nie posiadało skutecznych narzędzi zarządczych zapewniających nadzór nad BI. Brak dokumentowania spotkań Kierownictwa Biura z dyrektorami departamentów uniemożliwiał skuteczne monitorowanie i ocenę podjętych w ich wyniku decyzji i działań.

Jak wskazano[13], nadzór nad procesem zarządzania BI sprawowany był poprzez niedokumentowane spotkania Kierownictwa Biura z kierownictwem DOA i dyrektorami innych departamentów. W ocenie Kontrolowanego[14], Kierownictwo BRPP posiadało bieżącą wiedzę w zakresie procesów z obszaru BI, co pozwalało na właściwą reakcję w przypadku nieprawidłowości w tym przedmiocie.

Niezależnie od spotkań, zadaniem Kierownictwa Jednostki jest przyjęcie PBI i opracowanie adekwatnego SZBI. Tylko wtedy możliwe jest sprawowanie efektywnego nadzoru nad BI, w tym rozliczanie podjętych działań, ich monitorowanie oraz skuteczna ocena zmierzająca do doskonalenia BI.

3. [role i odpowiedzialność] Nie określono ról i odpowiedzialności głównych osób zaangażowanych w BI, za wyjątkiem Dyrektora DOA i zdefiniowania w *Polityce Ochrony Danych* ról ASI i jego zastępcy, a w *Instrukcji danych osobowych* roli administratora właściwego (nadzorującego działanie aplikacji/systemu). Niesprecyzowanie tak istotnych elementów skutkowało brakiem możliwości przypisania konkretnym osobom pełnej odpowiedzialności za rozwój i wdrażanie BI oraz określenia osób, które wspierały Kierownictwo w określaniu adekwatnych zabezpieczeń.

W ocenie Kontrolowanego[15] przyjęta praktyka w zakresie odpowiedzialności za poszczególne obszary BI sprowadzała się do *całościowego podejścia do kwestii SZBI*. Wg Biura zadania w tym zakresie realizowano zgodnie z bieżącą analizą zagrożeń i ryzyk dla BI, mimo braku wprowadzenia kompleksowych regulacji wewnętrznych. W regulaminie organizacyjnym[16] zadania Dyrektora DOA określono jako zarządzanie zasobami i infrastrukturą informatyczno-techniczną oraz systemami teleinformatycznymi.

Zgodnie z *Polityką Ochrony Danych* ASI to osoba odpowiadająca m.in. za nadzorowanie działania powierzonych jej systemów informatycznych oraz zarządzanie kontami i uprawnieniami użytkowników. W sytuacjach tego wymagających (w szczególności, jeśli ASI

[11] Pismo z 5 grudnia 2022 r., bez znaku.
[12] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2022 r. poz. 1876, t. j.). Wejście w życie 5 czerwca 2009 r. Natomiast przepisy ustawy ustanawiające BRPP weszły w życie 21 maja 2009 r.
[13] Pismo z 23 września 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[14] Pismo z 23 września 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[15] Pismo z 17 października 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[16] Regulamin organizacyjny dla Biura Rzecznika Praw Pacjenta stanowiący załącznik do Zarządzenia nr 1/2018 Rzecznika Praw Pacjenta z dnia 12 stycznia 2018 r. Zarządzenie weszło w życie z dniem podpisania, z mocą obowiązującą od 1 stycznia 2018 r.

nie może podjąć określonych czynności) zadania te wykonuje zastępca ASI. Natomiast według *Instrukcji danych osobowych*, administrator właściwy to pracownik wskazany przez ASI, nadzorujący działanie aplikacji/systemu.

W celu sprawnego zarządzania procesem BI konieczne jest wyznaczenie ogólnych i szczegółowych odpowiedzialności przypisanych do określonych stanowisk. To Kierownictwo Biura powinno przydzielić role i odpowiedzialności w zakresie wdrażania, utrzymywania i doskonalenia obszaru BI oraz, w przypadku ustanowienia SZBI, określić obowiązek przedstawiania Kierownictwu wyników jego działania.

4. [analiza stanu BI] Zastrzeżenia budzi fakt, że Biuro nie uwzględniło wszystkich informacji przekazanych w piśmie Szefa KPRM[17] dot. najważniejszych i najczęściej powtarzających się nieprawidłowości stwierdzonych w wyniku kontroli przeprowadzonych przez KPRM w zakresie *wykorzystania systemów teleinformatycznych do realizacji zadań publicznych*. Podjęte przez BRPP działania służące organizowaniu obszaru BI były niewystarczające. Ograniczono się do podstawowych elementów, tj. zwiększenia bezpieczeństwa służbowej poczty pracowników, wymiany urządzenia brzegowego oraz zmiany wymagań dot. długości haseł.

Negatywnie należy ocenić brak działań w kluczowych obszarach BI, w szczególności dot. prowadzenia okresowych analiz ryzyka, audytów w zakresie BI, bazy konfiguracji CMDB, szkoleń osób zaangażowanych w proces przetwarzania informacji oraz niedokonanie analizy stanu BI. Uniemożliwiło to zarządzanie posiadanymi aktywami, infrastrukturą przeznaczoną do ich przetwarzania oraz zminimalizowanie ryzyka dot. BI.

Zrealizowane działania służące poprawie BI dotyczyły[18]: przeniesienia całej poczty mailowej na usługę Office 365 firmy Microsoft wraz z uruchomieniem 2-składnikowego logowania[19] do usługi poprzez stronę internetową, wymiany urządzenia brzegowego firewall wraz z zakupem gwarancji aktualizacji oprogramowania dla urządzenia, zmiany w *Instrukcji danych osobowych* w zakresie wymagań dot. długości haseł dostępowych (hasła dłuższe i zawierające co najmniej 3 z 4 grup znaków: małe litery, wielkie litery, cyfry, znaki specjalne).

Powodem niezrealizowania przeglądu dokumentacji dot. BI była sytuacja związana z pandemią COVID-19. Jak wyjaśniono[20], konieczne było przekierowanie środków i działań na priorytetowe zadania pomocy pacjentom.

Nie można zgodzić się z Kontrolowanym w sprawie przyczyn braku przeglądu dokumentacji dot. BI. Rozporządzenie KRI weszło w życie w 2012 r., a *ustawa o informatyzacji* – w 2005 r. Natomiast BRPP funkcjonuje od 2009 r., zaś pandemia COVID-19 rozpoczęła się w 2020 r. Przed wybuchem pandemii Biuro powinno rozpocząć działania dot. wykonania analizy BI i ustalenia aktualnego stanu bezpieczeństwa informacji. Stanowiłoby to podstawę do ustanowienia SZBI, a Kierownictwo BRPP posiadałoby narzędzia zarządcze do podejmowania właściwych dla obszaru decyzji.

5. [analiza ryzyka] W Biurze nie prowadzono okresowych analiz ryzyka. Tym samym nie realizowano obowiązku określonego w § 20 ust. 2 pkt 3 Rozporządzenia KRI. Skutkowało to brakiem opracowania planu postępowania z ryzykiem i regulacji wewnętrznych w tym obszarze W konsekwencji BRPP pozbawione było informacji niezbędnych do proaktywnego zarządzania BI, w tym przeciwdziałania zagrożeniom oraz ograniczania skutków w przypadku zmaterializowania się ryzyk.

W BRPP nie uregulowano zasad przeprowadzania analizy ryzyka BI, a brak uregulowania tego obszaru argumentowano[21] tym, że Biuro nie dysponowało specjalistami w tym zakresie. Wprowadzono jedynie mechanizmy pozwalające ocenić działanie systemów i procedur, które dostarczały informacji o możliwych zagrożeniach, tj. co kwartał przeprowadzano

[17] Pismo z 11 czerwca 2019 r., znak: COA.WK.588.1.2019.MF.
[18] Pismo z 21 października 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[19] 2-składnikowe logowanie ma za zadanie zabezpieczenie poświadczeń użytkownika. Jego skutkiem jest wprowadzenie dodatkowych warstw uwierzytelniających, np. potwierdzenie operacji logowania na smartfonie.
[20] Pismo z 21 października 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[21] Pismo z 23 września 2022 r., znak: RzPP-DOA-WOR.091.3.2022.

sprawdzenie poprawności działania systemów informatycznych, a wyniki tego sprawdzenia zamieszczano w *Karcie kontroli sprawdzającej działanie systemów informatycznych w Biurze Rzecznika Praw Pacjenta* (dalej: *Karta kontroli sprawdzającej*).

Zebrane w trakcie analizy systemów i procedur informacje oraz dane były omawiane podczas spotkań wewnętrznych Departamentu Organizacyjno-Administracyjnego, a także odpraw Kierownictwa, tj. Rzecznika Praw Pacjenta z dyrektorami wszystkich komórek organizacyjnych. Działania te nie były dokumentowane, bo jak wskazano[22], wynikało to z braku wytycznych w tym przedmiocie. Następnie identyfikowano ryzyko oraz szacowano prawdopodobieństwo wystąpienia zagrożeń. W wyniku wspólnej dyskusji i ustaleń Kierownictwa Biura z dyrektorami departamentów planowano reakcję na ryzyko, a także jego monitorowanie i kontrolę. Czynności tych również nie dokumentowano.

Karty kontroli sprawdzającej nie można uznać za analizę ryzyka zgodną z § 20 ust. 2 pkt 3 Rozporządzenia KRI. Celem analizy ryzyka BI powinna być przede wszystkim ocena ryzyk związanych z utratą integralności, dostępności lub poufności informacji, a następnie określenie sposobu postępowania z ryzykiem. Ponadto analizą ryzyka należy objąć wszystkie aktywa Jednostki. Z kolei wspólne dyskusje i ustalenia Kierownictwa Biura nie mogą zostać ocenione, w szczególności dlatego, że nie były dokumentowane.

6. [audyt] W Jednostce nie wdrożono regulacji w zakresie przeprowadzania okresowych audytów wewnętrznych w zakresie BI, w tym monitorowania realizacji zaleceń. W okresie objętym kontrolą przeprowadzono jeden audyt, skupiając się na badaniu zagadnienia BI przy pracy na odległość. Tym samym nie objęto badaniem wszystkich obszarów BI, a wynikający z § 20 ust. 2 pkt 14 Rozporządzenia KRI obowiązek jego wykonania przynajmniej raz w roku, został naruszony.

Negatywnie należy ocenić niewdrożenie rekomendacji audytu.

Audyt pn. *Bezpieczeństwo informacji przy pracy na odległość*, realizowany był na przełomie 2020 r. i 2021 r. Na 2022 r. zaplanowano kolejne zadanie audytowe[23] dot. obszaru zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie[24].

Zakresem zrealizowanego audytu objęto kwestie związane z analizą ryzyka, podziałem zadań i urządzeniami wykorzystywanymi przy pracy na odległość, fizycznym bezpieczeństwem miejsca pracy, bezpieczeństwem kanału komunikacji, świadomością pracowników, kopiami zapasowymi i incydentami. Jednak zagadnienia te oceniono jedynie w odniesieniu do obszaru pracy na odległość. Audyt ten nie objął zatem swym zakresem wszystkich obszarów SZBI, w szczególności nie dotyczył on obszarów kompleksowego przeglądu SZBI, opracowania planu ciągłości działania, szkoleń, umów serwisu i rozwoju infrastruktury oraz systemów informatycznych, inwentaryzacji sprzętu i oprogramowania informatycznego, projektowania i wdrażania systemów teleinformatycznych, rozliczalności, zarządzania zmianą w systemie, zabezpieczeń organizacyjno-technicznych dostępu do informacji i systemów.

Wskazano[25], że audytowi podlegały jedynie wybrane elementy SZBI ze względu na ograniczone zasoby osobowe, tj. zatrudnienie audytora w wymiarze 1/5 czasu pracy. Do badania audytowego wybierany był obszar o najwyższym poziomie ryzyka wg opinii Dyrektora DOA i audytora wewnętrznego.

W sprawozdaniu z audytu[26] przedstawiono 8 rekomendacji. Termin realizacji większości zaleceń (tj. 6[27]) został wyznaczony do 31 grudnia 2023 r., co spowodowało, że audyt ten nie

[22] Pismo z 17 października 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[23] Pismo z 20 września 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[24] Obecnie przeprowadzana jest analiza i przegląd dokumentacji w celu sporządzenia wstępnych wyników audytu i przekazania ich do uzgodnienia z audytowanym.
[25] Pismo z 20 września 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[26] *Sprawozdanie z zadania audytowego nr 3/2020 „Bezpieczeństwo informacji przy pracy na odległość”*, z 8 czerwca 2021 r.
[27] **Z**alecenie 1 dot. dokonania analizy ryzyka w odniesieniu do pracy zdalnej.
Zalecenie 3 dot. dokonania podziału ról i odpowiedzialności za BI.
Zalecenie 4 dot. dokonania identyfikacji danych nieobjętych systemem automatycznego tworzenia kopii zapasowych oraz określenia sposobu i częstotliwości ich tworzenia.
Zalecenie 5 dot. określenia zakresu i częstotliwości testowania odtwarzania kopii zapasowych.
Zalecenie 6 dot. prowadzenia monitoringu ruchu sieciowego BRPP.
Zalecenie 8 dot. zdefiniowania i określenia sposobu zgłaszania zdarzeń i incydentów związanych z BI.

przyczynił się do usprawnienia zbadanego obszaru. Ponadto jedno[28] zalecenie zrealizowano po terminie, a inne[29], mimo upływu terminu na jego realizację, nie zostało zrealizowane.

Audyt wewnętrzny jako działalność niezależna i obiektywna ma celu wspieranie kierownika danej jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze[30]. Realizacja audytu w niepełnym zakresie, choć istotna, nie zapewnia pełnej oceny funkcjonujących rozwiązań w zakresie BI. Braku wykorzystania i wdrożenia przez Rzecznika BRPP rekomendacji uniemożliwił wyeliminowanie słabości i usprawnienie funkcjonowania Biura w obszarze BI.

7. [baza CMDB] BRPP nie utworzyło bazy konfiguracji CMDB zawierającej informacje o wszystkich zidentyfikowanych aktywach informatycznych, w tym szczegółowe dane o urządzeniach technicznych, oprogramowaniu i środkach komunikacji, ich rodzaju parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku. Stanowi to naruszenie § 20 ust. 2 pkt 2 Rozporządzenia KRI.

Biuro nie mogło efektywnie zarządzać infrastrukturą informatyczną, ponieważ ewidencjonowało wyłącznie komputery (stacjonarne oraz laptopy). Mimo że posiadane narzędzie (IT Manager) umożliwiało rejestrowanie zasobów informatycznych innych niż komputery. Ponadto wykorzystywany program posiadał funkcjonalność umożliwiającą tworzenie relacji pomiędzy umieszczonymi w bazie zasobami[31], jednak BRPP nie korzystało z tej możliwości.

Nie wprowadzono również regulacji wewnętrznych opisujących sposób zarządzania sprzętem informatycznym i oprogramowaniem oraz funkcjonowania rejestru zasobów informatycznych.

> Biuro nie utworzyło rejestru zasobów informatycznych (bazy konfiguracji CMDB). Zamiast tego, za pomocą programu IT Manager[32] prowadzono bazę użytkowanych komputerów stacjonarnych oraz laptopów. Baza ta nie zawierała informacji nt. użytkowanych w Biurze urządzeń mobilnych (smartfonów, tabletów), telefonów stacjonarnych, monitorów, sprzętu do wideokonferencji, drukarek, faxów, xero, skanerów, niszczarek, kart rozszerzeń, klawiatur, myszek, stacji dokujących, przenośnych napędów CD/DVD, pendrive'ów. Natomiast w odniesieniu do komputerów stacjonarnych i laptopów nie wprowadzono informacji dot. numeru inwentarzowego, daty zakupu oraz przypisanego użytkownika i fizycznej lokalizacji urządzenia.
>
> Baza użytkowanych sprzętów podlegała przeglądom raz na 1 lub 2 miesiące pod kątem aktualizacji w zakresie wprowadzonego sprzętu. W ocenie Kontrolowanego[33], posiadane narzędzia dawały możliwość zarządzania aktywami informatycznymi, a poprzez regularną ich aktualizację możliwy był nadzór nad nimi. Zdaniem Jednostki wprowadzone narzędzia i metody inwentaryzacji sprzętu były adekwatne do posiadanych możliwości budżetowych i kadrowych.

W bazie konfiguracji CMDB powinny znajdować się dane dot. wszystkich zasobów informatycznych (tj. nie tylko urządzeń technicznych, np. komputerów, ale również oprogramowania), a także informacje nt. relacji między nimi oraz ich użytkownikach. Należy się zgodzić z Kontrolowanym, że *posiadane narzędzia dawały możliwość zarządzania aktywami informatycznymi*, jednakże Biuro nie wykorzystywało w pełni narzędzia, które posiadało. Baza użytkowanych przez BRPP sprzętów zawierała wyłącznie komputery i aktywa te nie były przypisane ich właścicielom. Należy zaznaczyć, że działania związane ze stworzeniem bazy konfiguracji CMDB powinny być poprzedzone opracowaniem i wdrożeniem regulacji określających zakres przetwarzania danych dot. sprzętu i oprogramowania.

---

[28] Zalecenie 7 dot. przeprowadzenia szkolenia nt. zagrożeń podczas wykonywania pracy zdalnej.
[29] Zalecenie 2 dot. uregulowania organizacji pracy zdalnej.
[30] Definicja audytu wewnętrznego zawarta w art. 272 ust. 1 ustawy z dania 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022 r., poz. 1634 t. j. ze zm.).
[31] https://www.it-man.pl/funkcjonalnosc/zarzadzanie-zasobami/, dostęp: 17.11.2022 r.
[32] Program ten służy m. in. do inwentaryzacji konfiguracji komputerów oraz monitorowania użytkowników i zarządzania ich dostępem.
[33] Pismo z 5 października 2022 r., znak: RzPP-DOA-WOR.091.3.2022.

8. **[praca zdalna]** W dokumentach, tj. *Poleceniu pracodawcy w sprawie wykonywania pracy zdalnej* oraz *Instrukcji danych osobowych* określono kwestie dot. BI, ponieważ wskazano tam informacje nt. miejsca wykonywania zadań, zlecania i organizacji pracy zdalnej, odbioru wyników pracy, ewidencji czasu pracy i czynności wykonywanych zdalnie, praw i obowiązków pracowników i pracodawcy. Z kolei zagadnienia dot. nadawania uprawnień określono w *Instrukcji danych osobowych*. Dobrym rozwiązaniem było zamieszczenie w Intranecie prezentacji przedstawiającej zagadnienia związane z BI podczas pracy zdalnej.

Zastrzeżenia budzi fakt, że nie wskazano opisu wymaganych zabezpieczeń w przypadkach dopuszczenia możliwości korzystania z domowej sieci Wi-Fi.

> Praca zdalna była wykonywana na podstawie przepisów ustawy[34] oraz *Polecenia pracodawcy w sprawie wykonywania pracy zdalnej*, podpisywanego przez Dyrektora Generalnego. Pracownikom wykonującym pracę zdalnie zapewniono stałe wsparcie techniczne. Kwestie związane z nadawaniem uprawnień do korzystania ze sprzętu służbowego wynikały z *Instrukcji danych osobowych*. Ponadto w Intranecie BRPP udostępniono dla wszystkich pracowników prezentację pn. *Praca zdalna. O czym należy pamiętać?*, w której wyjaśniono zasady pracy zdalnej, w tym zagadnienia dot. BI (m. in. postępowanie ze służbowymi dokumentami, zabezpieczanie nośników danych, korzystanie ze służbowego Internetu i łączenie się z siecią za pośrednictwem VPN).

9. Pozytywnie należy ocenić, że Biuro wyposażyło swoich pracowników w służbowy sprzęt. Wszystkie urządzenia mobilne (95) w prawidłowy sposób zabezpieczano pod kątem uwierzytelniania użytkownika, bezpiecznego szyfrowania połączenia VPN oraz instalacji oprogramowania antywirusowego, którego bazę danych o wirusach aktualizowano automatycznie. Natomiast zastrzeżenia budzi, że systemem [redacted], tj. narzędziem do zabezpieczenia aplikacji i danych oraz kontroli urządzeń przenośnych, nie objęto 15 z 95 (16%) najstarszych z urządzeń. Nie wdrożono również narzędzi umożliwiających monitorowanie zdalnego dostępu pracowników do zasobów i systemów, co nie pozwalało na zapewnienie rozliczalności działań użytkowników.

> Wszyscy pracownicy świadczący pracę zdalną korzystali ze służbowego sprzętu[35]. Dostęp do zasobów następował przez bezpieczny tunel VPN. Kontrolujący wyjaśnił, że pracownicy pracujący zdalnie posiadali skonfigurowane urządzenia w taki sposób, aby zapewniały one dostęp do zasobów i systemów, jakie zostały przydzielone w przypadku świadczenia pracy w trybie stacjonarnym.
>
> Od grudnia 2020 r. większość urządzeń mobilnych (84%) objęto systemem [redacted]. Jego funkcjonalność polegała m. in. na: tworzeniu profili, zarządzaniu ograniczeniami, ustawianiu zasad dotyczących PIN i haseł, wymuszeniu ustawienia blokady ekranu, możliwości zdalnego przywrócenia zgubionego urządzenia do ustawień fabrycznych i usunięcia danych z urządzenia, blokowaniu możliwości przywracania do ustawień fabrycznych przez samych użytkowników. Poinformowano[36], że 15 najstarszych urządzeń mobilnych (na 95, tj. łączną liczbę wszystkich urządzeń mobilnych) nie objęto [redacted], ponieważ nie są one kompatybilne z tym systemem. Na przełomie listopada i grudnia 2022 r. urządzenia te mają zostać zastąpione przez nowe.
>
> W BRPP nie monitorowano bezpośrednio dostępu użytkowników świadczących pracę zdalnie do zasobów i systemów. Wykonywany był on jedynie incydentalnie, np. w zakresie czasu pracy pracowników poprzez kontrolę logowania się do systemu EZD PUW.

10. **[kopie zapasowe]** Konieczne jest wzmocnienie działań w zakresie wykonywania, przechowywania i testowania kopii zapasowych. Biuro dysponowało kopiami zapasowymi badanego systemu teleinformatycznego, tj. EZD PUW. Okres ich retencji był odpowiedni i wynosił 1 miesiąc. Prawidłowo dokumentowano działania związane z testowaniem kopii zapasowych, ale zasadnym byłoby zwiększenie częstotliwości ich testowania, tj. raz

---

[34] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. z 2020 r. poz. 374, t. j. ze zm.).
[35] Pismo z 22 września 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[36] Pismo z 21 października 2022 r., znak: RzPP-DOA-WOR.091.3.2022.

na miesiąc zamiast raz na kwartał, ponieważ zapewniłoby to większą regularność sprawdzania poprawności zapisu kopii. Ponadto niezbędne byłoby przeniesienie kopii zapasowych w inne miejsce niż to, w którym uruchomiony był EZD PUW.

W odniesieniu do EZD PUW wykonywano syntetyczne kopie zapasowe (full backup) raz w tygodniu ([redacted]). Były one tworzone z kopii inkrementalnych (przyrostowych) wykonywanych codziennie ([redacted]). Retencja przechowywania kopii została ustalona na 1 miesiąc – w przypadku kopii syntetycznych oraz na 1 tydzień – w przypadku kopii inkrementalnych.

Biuro nie dysponowało odpowiednim pomieszczeniem do przechowywania kopii zapasowych, ponieważ w tej samej lokalizacji znajdował się system teleinformatyczny EZD PUW. Brak przechowywania tych kopii w innej lokalizacji rodzi ryzyko niezapewnienia ich bezpieczeństwa w sytuacji uszkodzeń ośrodka podstawowego (serwerowni). Rzadkie testowanie kopii zapasowych (raz na kwartał, zamiast co miesiąc) wynikało[37] z przyjętej praktyki. Działania te były dokumentowane w *Karcie kontroli sprawdzającej*.

11. Regulacje wewnętrzne dotyczące wykonywania, przechowywania i testowania kopii zapasowych nie były aktualne oraz wymagały uzupełnienia i dostosowania do rozwiązań funkcjonujących w Biurze.

Ogólne postanowienia w zakresie kopii zapasowych zostały zawarte w *Instrukcji danych osobowych*, w szczególności dotyczyły one częstotliwości wykonywania kopii zapasowych oraz ich retencji. Natomiast w regulacji tej nie określono szczegółowych zasad związanych z zakresem (pełnym lub przyrostowym) ich wykonywania, przechowywania w innej lokalizacji, częstotliwości przeprowadzania testów związanych z odtworzeniem kopii zapasowych. Jak podano[38], brak uregulowania tych zagadnień wynikał z tego, że każdy z użytkowanych przez Jednostkę systemów[39] posiada odrębne potrzeby w zakresie backupu. Z tego względu w *Instrukcji danych osobowych* zamieszczono informacje ogólne, będące jedynie wytycznymi do zabezpieczania i wykonywania kopii zapasowych.

12. **[szkolenia]** Podjęte działania były niewystarczające, ponieważ w okresie objętym kontrolą szkolenie odbyło tylko 48 z 115 (42%) pracowników zatrudnionych na dzień 19 września 2022 r. Jednakże zdecydowaną większość z nich (tj. 47) przeszkolono w 2022 r., a jedynie 1 osobę (tj. Dyrektor DOA) w 2021 r. i 2022 r., przez co nie zapewniono cykliczności szkoleń. Ponadto nie przeszkolono wszystkich (tj. 40) stażystów, praktykantów i wolontariuszy. Dobrą praktyką było korzystanie przez pracowników z informacji dot. BI zamieszczanych w Intranecie, jednakże takie działanie powinno stanowić jedynie uzupełnienie w stosunku do szkoleń.

28 marca 2022 r. zrealizowano szkolenie on-line pn. *Nie daj się cyberzbójom*. Dyrektor Generalny BRPP zobowiązał[40] wszystkich pracowników do udziału w nim. Wynikało to z przyjętej w 2022 r. praktyki, aby szkolenia w zakresie BI odbywały się co najmniej raz w roku. Mimo to, przeszkolono jedynie 53[41] pracowników. Wyjaśniono[42], że w trakcie szkolenia 23 pracowników przebywało na urlopach, zwolnieniach lekarskich lub było długotrwale nieobecnych. Pozostali wykonywali w tym czasie inne obowiązki. Dodano, że nieprzeszkoleni zostaną ponownie zobowiązani do uczestnictwa w szkoleniu. Brak przeszkolenia stażystów, praktykantów i wolontariuszy argumentowano tym, że każda z tych osób podlega szkoleniu wstępnemu, którego zakres obejmuje również tematykę BI. Nie można zgodzić się z tym, ponieważ szkolenie to dotyczyło głównie zagadnień ochrony danych osobowych i nie obejmowało pozostałych obszarów BI.

Oprócz wspomnianego szkolenia, 2 pracownikom (Dyrektorowi DOA i administratorowi zasobów informatycznych) zapewniono inne szkolenia, tj. *V Forum Bezpieczeństwa IT w administracji*, *Studium bezpieczeństwa informacji i cyberbezpieczeństwa* oraz

[37] Pismo z 11 października 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[38] Pismo z 11 października 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[39] BRPP użytkuje, oprócz systemu teleinformatycznego EZD PUW, również systemy informatyczne, tj. RPP STAT, enova365, FINANSE PREMIUM.
[40] Pismo z 21 marca 2022 r., znak: RzPP-DFK-WKA.142.11.2022.
[41] W tym 6 pracowników, którzy na 19 września 2022 r. nie byli już pracownikami BRPP. 1 pracownik zatrudniony na 19 września 2022 r., tj. administrator zasobów informatycznych nie uczestniczył w tym szkoleniu. Natomiast wziął udział w szkoleniu pn. *Nowoczesne i bezpieczne środowisko IT*.
[42] Pismo z 27 września 2022 r., znak: RzPP-DOA-WOR.091.3.2022.

Nowoczesne i bezpieczne środowisko IT. Ponadto BRPP podejmowało dodatkowe działania informacyjne dla pracowników w zakresie BI. W Intranecie funkcjonowała zakładka *Bezpieczeństwo sieci*, w której znajdowały się m. in. informacje nt. najpopularniejszych zagrożeń w cyberprzestrzeni, sposobów zabezpieczania się przed zagrożeniami, czy odnośnik do strony internetowej zawierającej darmowy zestaw porad bezpieczeństwa dla użytkowników komputerów. Cyklicznie zamieszczano tam również wpisy z wiadomościami z zakresu BI.

13. W regulacjach wewnętrznych nie określono obowiązku organizacji szkoleń dla osób zaangażowanych w proces przetwarzania informacji. Nie wprowadzono również wymogu złożenia przez użytkowników oświadczenia o zobowiązaniu się do przestrzegania zasad dot. ochrony i BI.

Wskazano[43], że w BRPP obowiązuje zarządzenie Dyrektora Generalnego[44], umożliwiające planowanie szkoleń wynikających z przepisów ustawy o służbie cywilnej, a także innych szkoleń. W związku z tym nie wdrożono wytycznych w zakresie szkoleń użytkowników zaangażowanych w proces przetwarzania informacji. Ponadto w Biurze funkcjonuje jedynie wymóg złożenia *Oświadczenia osoby upoważnionej do przetwarzania danych osobowych*, a obowiązek złożenia oświadczenia o zobowiązaniu się do przestrzegania zasad dot. ochrony i BI zostanie wprowadzony w ramach planowanej dokumentacji SZBI.

Podnoszenie świadomości pracowników zmniejsza ryzyko popełnienia przez nich błędów i stanowi istotny element BI. Z tego względu ważne jest opracowanie zasad dotyczących zapewnienia im wiedzy, w tym gwarantujących cykliczność i dostępność różnych form szkoleń dla wszystkich pracowników.

Biorąc pod uwagę ustalenia i oceny przedstawione w *Wystąpieniu* oraz informacje zawarte w piśmie z 5 grudnia 2022 r.[45], zalecam:

1. Opracowanie i wdrożenie kompleksowego, spójnego systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność, integralność informacji, w tym:
- podstawowego dokumentu SZBI, tj. Polityki Bezpieczeństwa Informacji oraz pozostałych kompleksowych procedur zapewniających BI;
- wykonanie analizy BI i ustalenie aktualnego stanu bezpieczeństwa informacji, z uwzględnieniem informacji przekazanych w piśmie Szefa KPRM[46];
- ustanowienie ról i odpowiedzialności osób zaangażowanych w BI;
- przeprowadzenie rzetelnej analizy ryzyka w odniesieniu do wszystkich aktywów Jednostki wraz z opracowaniem planu postępowania z ryzykiem;
- utworzenie pełnej bazy konfiguracji CMDB;
- zwiększenie częstotliwości testowania odtworzenia kopii zapasowych.

2. Wdrożenie narzędzi i mechanizmów zarządczych gwarantujących Kierownictwu BRPP skuteczny nadzór w procesie ustanawiania, eksploatacji i doskonalenia SZBI.

3. Systematyczną ocenę funkcjonujących rozwiązań w zakresie BI, w szczególności poprzez realizację audytu oraz niezwłoczne wdrażanie jego rekomendacji.

4. Kontynuację działań mających na celu podnoszenie świadomości pracowników w obszarze BI oraz zapewnienie ich cykliczności.

5. Wyeliminowanie pozostałych nieprawidłowości wskazanych w Wystąpieniu.

---

[43] Pismo z 27 września 2022 r., znak: RzPP-DOA-WOR.091.3.2022.
[44] *Zarządzenie nr 24/2018 Dyrektora Generalnego Biura Rzecznika Praw Pacjenta z dnia 11 kwietnia 2018 r. w sprawie zasad organizacji i prowadzenia szkoleń oraz podnoszenia kwalifikacji zawodowych pracowników Biura Rzecznika Praw Pacjenta.*
[45] Bez znaku.
[46] Pismo z 11 czerwca 2019 r., znak: COA.WK.588.1.2019.MF.

Proszę o przedstawienie, w terminie 90 dni od daty otrzymania *Wystąpienia*, informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub o przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości.

Informuję, że od *Wystąpienia* nie przysługują środki odwoławcze.

Podstawa prawna:
Art. 46 ust. 3, art. 47, 48 i 49 *ustawy o kontroli*.

Z wyrazami szacunku
w zastępstwie
Szefa Kancelarii Prezesa Rady Ministrów

Andrzej Klarkowski
Podsekretarz stanu, zastępca szefa KPRM
/dokument podpisany elektronicznie/

Potwierdzam zgodność kopii wydruku z dokumentem elektronicznym:

Identyfikator dokumentu	260385.2186652.1905227
Nazwa dokumentu	wystąpienie pokontrolne BRPP KRI.pdf
Tytuł dokumentu	wystąpienie pokontrolne BRPP KRI
Sygnatura dokumentu	DNK.WK. 1741.6.2022.JG
Data dokumentu	28.12.2022
Skrót dokumentu	7A5BD829354E1D89478760E318EBEA81E65B426B
Wersja dokumentu	1.3
Data podpisu	28.12.2022 16:55:01
Podpisane przez	Andrzej Klarkowski Podsekretarz stanu, zastępca szefa KPRM
Rodzaj certyfikatu	Certyfikat kwalifikowany podpisu elektronicznego

EZD 3.109.303.303.

Data wydruku: 30.12.2022

Autor wydruku: Jankowski Tadeusz (Główny specjalista)