KANCELARIA PREZESA RADY MINISTRÓW
MINISTER – CZŁONEK RADY MINISTRÓW

Michał Dworczyk

COA.WK.583.12.2019.KD Warszawa, kwietnia 2020 r.

Pan
Tomasz Chróstny

Prezes
Urzędu Ochrony Konkurencji
i Konsumentów

WYSTĄPIENIE POKONTROLNE

Po rozpatrzeniu zastrzeżeń[1] złożonych do *Projektu wystąpienia pokontrolnego*, przedstawiam Panu Prezesowi *Wystąpienie pokontrolne* (dalej: *Wystąpienie*) z kontroli przeprowadzonej[2] przez Kancelarię Prezesa Rady Ministrów w Urzędzie Ochrony Konkurencji i Konsumentów[3] (dalej: UOKiK, Urząd lub Jednostka) w zakresie *wykonania zaleceń pokontrolnych dotyczących wykorzystania systemów teleinformatycznych do realizacji zadań publicznych* w okresie od 20 czerwca 2017 r. do 7 listopada 2019 r.

Podstawa prawna:
Art. 25 ust. 1 pkt 3 lit. b) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[4] (dalej: *ustawa o informatyzacji*) oraz art. 46 i 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[5] (dalej: *ustawa o kontroli*).

Zalecenia pokontrolne z czerwca 2017 r.

W czerwcu 2017 r.[6] obszar *wykorzystania przez UOKiK systemów teleinformatycznych do realizacji zadań publicznych* KPRM oceniła negatywnie i wydała zalecenia pokontrolne dotyczące:

1. Zapewnienia zgodności systemów teleinformatycznych z wymogami *ustawy o informatyzacji* oraz *Rozporządzenia KRI*.
2. Opracowania i wdrożenia spójnego systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji, w tym dostosowanie *Polityki bezpieczeństwa* do pełnego zakresu informacji gromadzonych i przetwarzanych w UOKiK.
3. Dokonania przeglądu wszystkich obszarów funkcjonowania Urzędu pod kątem możliwości wystąpienia potencjalnych ryzyk zagrażających bezpieczeństwu informacji oraz opracowania planu postępowania ze zidentyfikowanymi ryzykami.
4. Opracowania i wdrożenia zasad postępowania w kluczowych elementach projektowania, wdrażania, monitorowania oraz rozliczalności systemów teleinformatycznych.
5. Należytego zabezpieczenia interesów UOKiK w zawieranych umowach, w tym wprowadzenia i stosowania zasad pozwalających na rzetelne rozliczenie umów w oparciu o ich rzeczywisty, a nie szacunkowy zakres realizacji.
6. Wyeliminowania pozostałych nieprawidłowości wskazanych w *Wystąpieniu pokontrolnym*.

---

[1] Pismo z dnia z 6 marca 2020 r., znak: BP-4.0910.1.2019.
[2] Kontrolę przeprowadzili: p. Magda Jarosławska, główny specjalista, kierownik zespołu kontrolującego, p. Krzysztof Jakubczyk, główny specjalista, członek zespołu kontrolującego. Czynności kontrolne przeprowadzono w okresie od 7 listopada do 6 grudnia 2019 r., w siedzibie UOKiK w Warszawie, przy Pl. Powstańców Warszawy 1. Kontrolerzy spełniają wymogi określone w art. 28 ust. 1 *ustawy o informatyzacji*, w tym posiadają jeden z certyfikatów wymienionych w załączniku do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych (Dz. U. Nr 177, poz. 1195).
[3] UOKiK działa na podst. ustawy z 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r. poz. 369, t. j. ze zm.), Zarządzenia Nr 146 Prezesa Rady Ministrów z 23 grudnia 2008 r. w sprawie nadania statutu UOKiK (M. P. z 2018 r., poz. 208, j. t. ze zm.) oraz Zarządzenia Nr 23/2018 Prezesa UOKiK z 13 września 2018 r. *w sprawie nadania regulaminu organizacyjnego UOKiK*. Prezes UOKiK jest centralnym organem administracji rządowej, do którego kompetencji należy kształtowanie polityki antymonopolowej i polityki ochrony konsumentów, opiniowanie projektów pomocy publicznej, monitorowanie wsparcia udzielanego przedsiębiorcom oraz przygotowanie, na podstawie sprawozdań podmiotów udzielających pomocy oraz jej beneficjentów, rocznych raportów o wsparciu państwa.
[4] Dz. U. z 2020 r., poz. 346 t. j.
[5] Dz. U. z 2020 r., poz. 224 t. j.
[6] Wystąpienie pokontrolne Szefa Kancelarii Prezesa Rady Ministrów z 20 czerwca 2017 r., znak: COA.WK.583.8.2017.AB.

Za wdrożenie zaleceń pokontrolnych KPRM odpowiedzialne było od 15 marca 2018 r. Biuro Prezesa[7] (dalej: BP), we wcześniejszym okresie od 20 czerwca 2017 r. do 14 marca 2018 r. Biuro Budżetu i Administracji[8]. Natomiast administrowanie Systemem Harmonogramowania Rejestracji i Monitorowania Pomocy (dalej: SHRIMP) w całym okresie objętym kontrolą należało do kompetencji Departamentu Monitorowania Pomocy Publicznej[9].

OCENA KONTROLOWANEGO OBSZARU

Ponowna ocena wskazuje na konieczność intensyfikacji działań UOKiK w celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych i informacji gromadzonych i przetwarzanych w systemach teleinformatycznych wykorzystywanych do realizacji zadań publicznych. Pomimo upływu ponad dwóch lat od wydania zaleceń pokontrolnych KPRM, nie zrealizowano w pełnym zakresie żadnego z nich, tym samym nie usprawniono funkcjonowania Urzędu w istotnym obszarze.

System zarządzania bezpieczeństwem informacji (obszar wymaga istotnego wzmocnienia)

- **[SZBI]** Działania Urzędu w celu opracowania kompleksowego i spójnego systemu zarządzania bezpieczeństwem informacji (dalej: *SZBI*) gwarantującego poufność, dostępność i integralność przetwarzanych danych były nieskuteczne. Mimo negatywnej oceny tego obszaru podczas poprzedniej kontroli, wdrożenie kluczowych zaleceń wciąż znajduje się w początkowej fazie i wymaga wprowadzenia dalszych systemowych rozwiązań i usprawnień. W szczególności dotyczy to opracowania całościowej dokumentacji, która jest warunkiem skutecznego zarządzania bezpieczeństwem informacji. UOKiK nie dysponował najważniejszym i podstawowym dokumentem *SZBI* jakim jest *Polityka Bezpieczeństwa Informacji.*
- **[Nadzór]** Urząd nie posiadał skutecznych narzędzi zarządczych i mechanizmów zapewniających nadzór nad podejmowanymi działaniami w zakresie realizacji zaleceń pokontrolnych. W konsekwencji Kierownictwo UOKiK nie dysponowało bieżącymi informacjami i w niewystarczającym stopniu weryfikowało postęp prac w obszarze wdrażania *SZBI*.
- **[Strategia, analiza ryzyka i plan postępowania z ryzykiem]** Nie opracowano strategii rozwoju systemów informatycznych, dzięki której możliwe byłoby określenie priorytetów w zakresie rozbudowy oraz utrzymania systemów teleinformatycznych służących sprawnej realizacji zadań. Nie przeprowadzono także kompleksowej analizy ryzyka utraty integralności, dostępności i poufności informacji, która stanowi fundamentalną część procesu zarządzania ryzykiem. W rezultacie nie można stwierdzić, czy podejmowane działania były odpowiedzią na najistotniejsze, zidentyfikowane zagrożenia. W konsekwencji nieopracowania ww. analizy Urząd nie posiadał również planu postępowania z ryzykiem.
- **[Baza CMDB]** Wprowadzone rozwiązania w zakresie zarządzania infrastrukturą informatyczną wymagają usprawnień, bowiem wykorzystywane w tym celu narzędzie nie posiada w szczególności informacji nt. użytkowanego sprzętu niepracującego w sieci UOKiK.
- **[Zapewnienie wiedzy pracownikom]** Kontynuacji wymaga również edukacja pracowników nt. nowych zagrożeń, adekwatnych zabezpieczeń, skutków ewentualnych incydentów naruszenia bezpieczeństwa informacji. Szkolenia w tym zakresie zorganizowano dla 38% pracowników (195 z 512[10]). W dalszym ciągu nie wdrożono zasad dotyczących zarządzania wiedzą w ww. obszarach.

[7] Zgodnie z zarządzeniami DG UOKiK *w sprawie wewnętrznego regulaminu organizacyjnego Biura Prezesa*: Nr 8/2018 z 15 marca 2018 r., Nr 42/2018 z 24 lipca 2018 r., Nr 49/2018 z 27 września 2018 r., Nr 13/2019 z 13 sierpnia 2019 r.
[8] Zgodnie z zarządzeniami DG UOKiK *w sprawie wewnętrznego regulaminu organizacyjnego Biura Budżetu i Administracji*: Nr 16/2017 z 8 marca 2017 r., Nr 51/2017 z 17 sierpnia 2017 r. oraz Nr 9/2018 z 15 marca 2018 r.
[9] Zgodnie z zarządzeniami DG UOKiK *w sprawie wewnętrznego regulaminu organizacyjnego Departamentu Monitorowania Pomocy Publicznej:* Nr 7/2017 z 28 lutego 2017 r. oraz Nr 37/2018 z 24 lipca 2018 r.
[10] Wg stanu zatrudnienia na dzień 7 listopada 2019 r.

- **[SHRIMP, SHRIMPv2 oraz procedury]** Pozytywnie należy ocenić, że UOKiK podjął adekwatne działania do możliwości funkcjonalnych SHRIMP w celu jego dostosowania do wymogów *Rozporządzenia KRI*[11], a wobec braku możliwości zapewnienia pełnej zgodności wdraża nową wersję systemu SHRIMPv2. Wsparcia wymagają jednak regulacje wewnętrzne w zakresie projektowania, wdrażania oraz wprowadzania zmian w systemach teleinformatycznych.
- **[Umowy]** W umowach na obsługę i utrzymanie systemów teleinformatycznych nie stosowano postanowień, które stanowiłyby należyte zabezpieczenie interesów UOKiK. Nie wprowadzono zasad pozwalających na rzetelne rozliczenie umów w oparciu o rzeczywisty a nie szacunkowy zakres realizacji przedmiotu umowy.
- **[Serwerownia]** Podjęto działania w zakresie poprawy bezpieczeństwa serwerowni poprzez jej przeniesienie do pomieszczenia o wyższym standardzie. Jednakże w nowym pomieszczeniu nadal nie usunięto w całości braków w stanie wyposażenia.
- **[Kopie zapasowe]** UOKiK wykonywał i testował kopie zapasowe, a także prowadził testowanie aktualizacji systemów i oprogramowania na dedykowanym do tego celu środowisku testowym. Działania te podjęto w 2019 r. po dokonaniu przez Urząd zakupu specjalistycznego sprzętu.
- **[Plan ciągłości działania]** Pomimo stwierdzenia w poprzedniej kontroli nieprawidłowości w zakresie braku planu ciągłości działania na wypadek wystąpienia zdarzeń o niskim prawdopodobieństwie, ale o katastrofalnych skutkach, takich jak np. pożar, katastrofa budowlana, terroryzm, powódź, dokument taki nie został opracowany.
- **[Rozliczalność działań]** Nie wyeliminowano nieprawidłowości dot. niezapewnienia rozliczalności działań prowadzonych w systemach teleinformatycznych. Nie wdrożono procedur w tym przedmiocie, w szczególności określających zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych. Ponadto nie prowadzono regularnych przeglądów informacji zawartych w dziennikach systemowych w celu wykrycia nieuprawnionego dostępu lub działań niepożądanych.

Wymiana informacji w postaci elektronicznej

Nie opracowano procedur określających deklarowany poziom dostępności dostarczanych usług przez systemy teleinformatyczne, o których mowa w § 15 ust. 2 *Rozporządzenia KRI*.

Zapewnienie dostępności informacji zawartych na stronie internetowej

Pozytywnie należy ocenić, że Urząd dostosował stronę internetową do wymagań określonych w § 19 *Rozporządzenia KRI*, przez co zapewnił jej dostępność dla osób z niepełnosprawnościami.

OCENY I USTALENIA SZCZEGÓŁOWE

I. System zarządzania bezpieczeństwem informacji

1. [stan SZBI] Negatywnie należy ocenić, że UOKiK nie zrealizował najistotniejszego zalecenia pokontrolnego KPRM dotyczącego wdrożenia spójnego *SZBI*, pomimo zadeklarowania[12] jego utworzenia w terminie do końca 2018 r.[13] oraz upływu ponad 28 miesięcy od sformułowania zalecenia. Jednostka nie dysponowała podstawowym dokumentem *SZBI* jakim jest *Polityka Bezpieczeństwa Informacji* (dalej: *PBI* lub *Polityka*), a jej wdrożenie zaplanowano dopiero na koniec I kw. 2020 r.

[11] 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.).
[12] Pismo z 16 października 2017 r., nr: BBA-071-03(88)/17(MI) dotyczące sposobu wykonania zaleceń pokontrolnych.
[13] Z wyjątkiem wdrożenia systemu SHRIMP oraz usunięcia braków w stanie wyposażenia serwerowni, które miały zostać zrealizowane do 2020 r.

W UOKiK z dniem 1 września 2017 r. zostały wdrożone *Polityka Przetwarzania Danych Osobowych* oraz *Instrukcja Zarządzania Systemem Informatycznym*[14], jednakże regulacje te nie stanowiły kompleksowych uregulowań *SZBI*, ponieważ skupiały się głównie na ochronie danych osobowych. Zgodnie z wyjaśnieniami[15], w Urzędzie dokonano wielu zmian organizacyjnych, w szczególności związanych z przesunięciem Wydziału Informatyki z Biura Budżetu i Administracji do Biura Prezesa, jak i strukturalnych, mających służyć szybszemu opracowaniu *PBI*. Ponadto wskazano, że zrealizowano projekty informatyczne, które odpowiadały na pilne potrzeby UOKiK, jednakże przyczyniły się one do wydłużenia czasu wdrożenia *PBI*. W opinii Urzędu, pomimo niewdrożenia *PBI*, wykonano szereg działań na rzecz podniesienia bezpieczeństwa informacji, w szczególności zakupiono i wdrożono system backupowy, technologię zabezpieczającą przed dostępem do sieci Urzędu obcych komputerów, oprogramowanie do centralnego zarządzania switchami, wymieniono urządzenia firewall, zlecono konserwację wszystkich kluczowych urządzeń UPS. Obecnie wdrażany jest nowy serwer pocztowy oraz instalowane oprogramowanie zabezpieczające przed wyciekiem wrażliwych danych z Urzędu.

Ustanowienie *SZBI* zapewniającego poufność, dostępność i integralność informacji wymaga opracowania kompleksowych regulacji wewnętrznych, które zagwarantują sprawność działania systemu. Dlatego prace nad ich wdrożeniem powinny przebiegać niezwłocznie i efektywnie, tymczasem w UOKiK pierwszy projekt *PBI* opracowany został dopiero po ponad roku od wydania zaleceń pokontrolnych KPRM.

Prace nad projektem *PBI* rozpoczęły się jesienią 2017 r. i toczyły się interdyscyplinarnie z udziałem kilku komórek organizacyjnych. W wyniku współpracy po roku, tj. jesienią 2018 r., przygotowano projekt *Polityki*, który został skierowany do pierwszych konsultacji[16]. Dopiero 27 listopada 2018 r.[17], tj. 17 miesięcy po wydaniu zaleceń KPRM, powołano *Zespół ds. SZBI*, który kontynuował czynności związane z opracowaniem *PBI*, korzystając z efektów wcześniejszej współpracy komórek organizacyjnych Jednostki.

Bezpieczeństwo informacji wymaga podejmowania niezwłocznych działań korygujących, a całościowa dokumentacja *SZBI* jest niezbędnym warunkiem skutecznego zarządzania tym obszarem. Ponadto zależy ono od świadomości pracowników, w związku z tym tak ważne jest przejrzyste i kompleksowe określenie zasad w tym zakresie.

2. [przegląd i plan] W UOKiK nie wdrożono narzędzi zarządczych pozwalających na efektywne utworzenie spójnego *SZBI*. W szczególności nie przeprowadzono przeglądu rozwiązań funkcjonujących w Jednostce w zakresie bezpieczeństwa informacji, zapewniającego identyfikację zarówno obszarów wymagających usystematyzowania i wdrożenia nowych zasad/procedur, jak i tych, w przypadku których istnieje potrzeba podjęcia działań naprawczych. Ponadto nie monitorowano skutecznie postępu w zakresie realizacji zaleceń pokontrolnych KPRM.

Obowiązek wykonania przeglądu należał do *Zespołu ds. SZBI*, który miał w szczególności weryfikować i aktualizować obowiązujące akty prawne w zakresie bezpieczeństwa informacji, opracowywać projekty regulacji wewnętrznych, w tym dokonywać przeglądu i optymalizacji procesów. Przegląd nie został przeprowadzony, gdyż, jak wyjaśniono[18], *przegląd i optymalizacja procesów była podejmowana w trybie roboczym od 2017 r. Zespół nie powielał tych działań, koncertując się na przygotowaniu projektów dokumentów wdrażających PBI i Politykę Bezpieczeństwa Ochrony.*

Ponadto nie monitorowano skutecznie realizacji zaleceń pokontrolnych KPRM. Wyjaśniono[19], że zestawienie przekazane po kontroli KPRM[20] wraz z postępem prac jest na bieżąco aktualizowane, a dokument z racji częstej ewaluacji ma charakter roboczy, wewnętrzny, niemniej wciąż wiążący. Jednakże wskazać należy, że odpowiedź przekazana Szefowi KPRM nie mogła stanowić skutecznego narzędzia do ww. monitoringu, bowiem nie zawierała informacji nt. wyeliminowania wszystkich nieprawidłowości. W szczególności brak było danych nt. realizacji przeglądów *SZBI*, nieefektywnego usytuowania Wydziału Informatyki w UOKiK, rozwiązania problemu połączonych

[14] Zał. Nr 1 i 2 do zarządzenia Nr 19/2017 Prezesa UOKiK z 1 sierpnia 2017 r., zmienione zarządzeniami: Nr 14/2018 z 24 maja 2018 r. i Nr 9/2019 z 12 marca 2019 r.
[15] Pismo Za-cy Dyrektora BP z 22 listopada 2019 r., nr: BP-4.0910.1.2019.
[16] Wyjaśnienia Za-cy Dyrektora BP z 21 listopada 2019 r., nr: BP-4.0910.1.2019.
[17] Zarządzenie Nr 26/2018 Prezesa UOKiK z 27 listopada 2018 r. *w sprawie powołania Zespołu do spraw Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Ochrony Konkurencji i Konsumentów* (dalej: zarządzenie w sprawie powołania Zespołu ds. SZBI).
[18] Pismo Za-cy Dyrektora BP z 3 grudnia 2019 r., nr: BP-4.0910.1.2019.
[19] Pismo Za-cy Dyrektora BP z 29 listopada 2019 r., nr: BP-4.0910.1.2019.
[20] Odpowiedź na wystąpienie pokontrolne dot. sposobu realizacji zaleceń – pismo z 16 października 2017 r., nr: BBA-071-03(88)/17(MI).

uprawnień administratora systemu i użytkownika merytorycznego, uszczegółowia procedury o informacje nt. osób odpowiedzialnych za realizację działań w przypadku ujawnienia wirusa, nieprowadzenia testowania aktualizacji na dedykowanym do tego celu środowisku testowym, opracowania planów ciągłości działania oraz procedury określającej deklarowany poziom dostępności dostarczanych usług elektronicznych.

Efektywne wdrażanie *SZBI* powinno rozpocząć się od diagnozy istniejących rozwiązań w organizacji, co umożliwia przegląd *SZBI*. Następnie, aby móc monitorować jego tworzenie, powinien powstać plan wdrażania ww. systemu, zawierający w szczególności planowane działania, termin ich wdrożenia oraz osoby odpowiedzialne za ich realizację. Kompleksowa identyfikacja słabości i jego opracowanie przyczyniłyby się niewątpliwie do skutecznego zarządzania ww. obszarem.

3. [nadzór Kierownictwa] W Jednostce nie wprowadzono skutecznych rozwiązań zapewniających nadzór nad podejmowanymi działaniami w zakresie bezpieczeństwa informacji. Tym samym Kierownictwo UOKiK w niewielkim stopniu weryfikowało postęp prac w zakresie wdrażania spójnego systemu *SZBI*.

Dyrektor Generalny UOKiK (dalej: DG UOKiK) kilkukrotnie[21] zwracał się do BP o udzielenie wyjaśnień nt. stanu wdrażania zaleceń pokontrolnych KPRM. Jednakże otrzymał ogólne informacje nt. zmian organizacyjnych, tj. umiejscowienia Wydziału Informatyki w strukturach Biura Prezesa, opracowaniu projektu zarządzenia w sprawie powołania *Zespołu ds. SZBI* oraz projektu *PBI*[22], a co istotne część korespondencji pozostała bez odpowiedzi[23].

W opinii Urzędu[24], narzędziem zapewniającym nadzór nad wprowadzaniem *SZBI* było powołanie *Zespołu ds. SZBI*. Jego Przewodniczący zobowiązany[25] był m.in. do przedstawienia Kierownictwu UOKiK raportu z prac za rok poprzedni wraz z rekomendacjami oraz propozycji działań i planu wydatków związanych z realizacją zadań dot. zapewnienia bezpieczeństwa informacji. Dokumenty te nie zostały jednak sporządzone, gdyż, jak wskazano[26], regulacje wewnętrzne nie definiują formy przedstawienia informacji, a założenia dot. harmonogramu prac, budżetu projektu, czy potrzeb szkoleniowych zostały przedstawione ustnie.

Działania w ramach tego systemu powinny być podejmowane w sposób ciągły i dokumentowane. Brak formy pisemnej uniemożliwia analizę i ocenę wdrażanych rozwiązań, a w dalszej kolejności również podejmowanie adekwatnych decyzji przez Kierownictwo Urzędu.

4. [strategia rozwoju] UOKiK nie wyeliminował nieprawidłowości w zakresie braku opracowania i zatwierdzenia strategii rozwoju systemów informatycznych. Stanowiłaby ona dokument łączący planowane działania w zakresie rozbudowy i utrzymania systemów teleinformatycznych z zadaniami powierzonymi dla Urzędu.

Główne cele rozwojowe w tym obszarze wprowadzane były do planów działalności UOKiK. Na lata 2017-2018 uwzględniono w nich modernizację systemu gromadzenia danych o udzielanej pomocy (SHRIMP). Została ona zrealizowana częściowo, ponieważ 1 września 2018 r. ogłoszono przetarg, jednak z uwagi na liczne zapytania i odwołanie do Krajowej Izby Odwoławczej podpisanie umowy z wykonawcą nastąpiło dopiero 6 maja 2019 r. Natomiast w 2019 r. zaplanowano m.in. wdrożenie systemu Skype, które udało się zrealizować. Ponadto wydatki związane z rozwojem systemów informatycznych uwzględniane były *w Planach postępowań o udzielenie zamówień publicznych, jakie UOKiK przewiduje przeprowadzić* w latach 2017-2019. W ocenie UOKiK[27], dokumenty te spełniły swoją rolę, bowiem w latach 2017-2019 wdrożono szereg mechanizmów, które przyczyniły się do rozwoju technologicznego organizacji, a tym samym do podniesienia poziomu bezpieczeństwa informacji. Wskazano, że jednolity dokument zawierający strategię rozwoju systemów informatycznych nie powstał, niemniej prace nad nim trwają i zostaną ukończone w 2020 r.

---

[21] Pisma z: 10 kwietnia 2018 r., nr: BKSiO-0910-1/18(29)/MS; 23 kwietnia 2018 r., nr: BKSiO-0910-1/18(33)/JO; 10 sierpnia 2018 r., nr: BKSiO-0910-1/18(39)MS; 12 września 2018 r., nr: BKSiO-0910-1/18(42)/(MS) oraz 16 października 2019 r., nr: BKSiO-4.0910.1.2019 (pismo skierowane do kilku komórek, w tym m.in. BP), a także e-maile z: 18 czerwca 2018 r. oraz 6 listopada 2018 r.

[22] Pisma z: 19 kwietnia 2018 r., nr: BP-0911-01/18(5); 25 kwietnia 2018 r., nr: BP-0911-01/18(7) oraz 12 września 2018 r., nr: BP-0911-1(18)/18.

[23] Bez odpowiedzi pozostały pisma z 10 sierpnia 2018 r., nr: BKSiO-0910-1/18(39)MS; 12 września 2018 r., nr: BKSiO-0910-1/18(42)/(MS) oraz 16 października 2019 r., nr: BKSiO-4.0910.1.2019, a także e-maile z: 18 czerwca 2018 r. oraz 6 listopada 2018 r.

[24] Pismo Za-cy Dyrektora BP z 29 listopada 2019 r., nr: BP-4.0910.1.2019.

[25] Postanowienia § 4 zarządzenia w sprawie powołania *Zespołu ds. SZBI*.

[26] Pismo Za-cy Dyrektora BP z 3 grudnia 2019 r., nr: BP-4.0910.1.2019.

[27] Załącznik do pisma Za-cy Dyrektora BP z 15 listopada 2019 r., nr: BP-4.0910.1.2019 oraz pismo Za-cy Dyrektora BP z 18 grudnia 2019 r., nr: BP-4.0910.1.2019.

Ww. dokumenty nie stanowiły kompleksowej strategii rozwoju systemów informatycznych zapewniającej wydajne wykorzystanie istniejących zasobów, ponieważ nie zawierały informacji nt. identyfikacji potrzeb wszystkich komórek organizacyjnych w tym obszarze, ustalenia priorytetów i wymagań, harmonogramu planowanych działań oraz osób odpowiedzialnych za ich wdrożenie.

5. [analiza ryzyka] Urząd mimo stwierdzenia w poprzedniej kontroli nieprawidłowości dot. braku analizy ryzyka nie podjął skutecznych działań w celu jej przeprowadzenia. Sporządzona mapa ryzyka nadal nie spełnia wymogów *Rozporządzenia KRI*, ponieważ nie odnosi się do wszystkich aktywów Jednostki, jak również nie została opracowana w zakresie ryzyk związanych z utratą integralności, dostępności i poufności informacji. UOKiK w dalszym ciągu nie posiada także planu postępowania z ryzykiem oraz regulacji wewnętrznych opisujących sposób zarządzania ryzykiem.

> W Jednostce przeprowadzono cykl warsztatów szkoleniowych dot. identyfikacji, analizy i postępowania z ryzykiem dla wszystkich komórek, w ich wyniku opracowana została mapa ryzyka. Nie spełniała ona jednak wymogów § 20 ust. 2 pkt 3 *Rozporządzenia KRI*, bowiem nie została przeprowadzona w odniesieniu do wszystkich aktywów UOKiK w zakresie ryzyk związanych z utratą integralności, dostępności i poufności informacji. Wyjaśniono[28], że na mapie ryzyk uwzględniono te dostrzeżone na danym etapie analizy oraz zadeklarowano, że w ramach *SZBI* dokonany zostanie przegląd ryzyk w obszarze bezpieczeństwa informacji, zgodnie z wytycznymi ww. Rozporządzenia. W odniesieniu do braku regulacji wskazano[29], że planowane jest uwzględnienie analizy ryzyka w dokumentacji *SZBI* oraz horyzontalnie w regulaminie organizacyjnym Urzędu, który miał zacząć obowiązywać od 1 stycznia 2020 r.

W celu utworzenia skutecznego *SZBI* Jednostka powinna zastosować zabezpieczenia gwarantujące bezpieczeństwo informacji adekwatne do poziomu ryzyka wynikającego z analizy ryzyka. Z tych względów w celu zapewnienia skuteczności wdrożonych zabezpieczeń, istotnym jest przeprowadzenie rzetelnej analizy ryzyka i opracowanie planu postępowania z ryzykiem, a następnie kontynuowanie systematycznego podejścia do zarządzania ryzykiem. Brak kompleksowej analizy zagrożeń związanych z przetwarzaniem informacji utrudnia proaktywne zarządzanie bezpieczeństwem informacji, w tym przeciwdziałanie zagrożeniom oraz ograniczanie skutków w przypadku zmaterializowania się ryzyk.

6. [audyt] Po kontroli KPRM w 2017 r. przeprowadzono audyt wewnętrzny bezpieczeństwa informacji, wypełniając obowiązek określony w § 20 ust. 2 pkt 14 *Rozporządzenia KRI*, jednakże nie wprowadzono mechanizmów zapewniających niezwłoczne wdrażanie jego zaleceń. Do dnia rozpoczęcia czynności kontrolnych zalecenia z audytu nie zostały zrealizowane.

> Od 12 lipca do 31 sierpnia 2017 r. w Urzędzie przeprowadzono audyt wewnętrzny bezpieczeństwa informacji[30]. Wyniki audytu były zbieżne z ustaleniami kontroli KPRM i potwierdziły pilną potrzebę wdrożenia działań korygujących. Zalecenia z audytu nie zostały jednak zrealizowane, co potwierdzały również czynności sprawdzające wskazując na konieczność kontynuowania działań monitoringu. Wyjaśniono[31], że w 2019 r. działania te nie zostały zakończone, a przez wzgląd na wieloaspektowość obszaru, będą ponawiane w 2020 r. do czasu ukończenia wdrażania *SZBI*.

7. [baza CMDB] Urząd wdrożył narzędzie pozwalające na zarządzanie sprzętem i oprogramowaniem, jednakże nie zapewniało ono kompletnej inwentaryzacji aktywów informatycznych. Narzędzie nie zawierało informacji nt. UPS-ów, kopiarek, drukarek, skanerów (bądź urządzeń wielofunkcyjnych), tabletów, telefonów oraz sprzętu niepracującego w sieci UOKiK. Tym samym Jednostka wciąż nie posiada narzędzia do skutecznego zarządzania infrastrukturą informatyczną spełniającego wymóg określony w § 20 ust. 2 pkt 2 *Rozporządzenia KRI*. Nie wdrożono również zasad zarządzania sprzętem, oprogramowaniem i jego konfiguracją.

---

[28] Pismo Za-cy Dyrektora BP z 3 grudnia 2019 r., nr: BP-4.0910.1.2019.
[29] Pismo Za-cy Dyrektora BP z 21 listopada 2019 r., nr: BP-4.0910.1.2019.
[30] Pn. *Ocena systemu zarządzania bezpieczeństwem informacji określonego w regulacjach wewnętrznych UOKiK*, sprawozdanie sporządzono 10 listopada 2017 r.
[31] Pismo Za-cy Dyrektora BP z 3 grudnia 2019 r., nr: BP-4.0910.1.2019.

Inwentaryzacja sprzętu i oprogramowania do przetwarzania informacji prowadzona była przy użyciu programu nVision. Program ten zawierał informacje o rodzaju, parametrach, aktualnej konfiguracji i relacjach między elementami konfiguracji oraz użytkowniku jedynie w odniesieniu do sprzętu podłączonego do sieci UOKiK. Brak było zatem danych nt. sprzętu niepracującego w sieci, w szczególności przeznaczonego do organizacji szkoleń/konferencji, utylizacji, naprawy bądź ponownego użytku. Ewidencja w tym zakresie prowadzona była w pliku Microsoft Excel, jednakże nie obejmowała ona danych w zakresie rodzaju sprzętu, oprogramowania i aktualnej konfiguracji, a w przypadku części sprzętu, również informacji w zakresie użytkownika. Natomiast UPS-y, kopiarki, drukarki, skanery (bądź urządzenia wielofunkcyjne), tablety i telefony ewidencjonowane były przez Biuro Budżetu i Administracji, zgodnie z prowadzonymi zapisami księgi inwentarzowej na potrzeby rachunkowości. Wyjaśniono[32], że *UPS-y, telefony i tablety nie pracują w sieci komputerowej i dlatego nie są widoczne w nVision. Zasada ta dotyczy także komputerów do sieci niepodłączonych*. Ponadto wskazano, że nie wprowadzono odrębnej regulacji do monitorowania zmian w środowisku teleinformatycznym, ale zasady te zostaną opisane w dokumentacji *SZBI*.

Podkreślić należy, że rejestr zasobów informatycznych nie jest tożsamy z danymi księgi inwentarzowej dla potrzeb rachunkowości[33]. Ponadto brak pełnej, aktualnej informacji o stanie aktywów informatycznych uniemożliwia przeprowadzenie rzetelnej analizy ryzyka i przygotowanie pełnego planu postępowania z ryzykiem. Utrudnia to również wprowadzanie zmian w środowisku teleinformatycznym.

8. [incydenty] Niezwłocznie po kontroli KPRM przeprowadzonej w 2017 r. rozpoczęto prowadzenie rejestru incydentów, jednakże zarządzanie zdarzeniami nie było wspierane przez regulacje wewnętrzne. Wdrożona *Instrukcja zarządzania systemem informatycznym* odnosiła się do postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych i nie regulowała zagadnień dotyczących analizy, nadawania priorytetów, wyszukiwania powiązań, podejmowania działań naprawczych, zakresu informacji podlegających obowiązkowi rejestracji oraz maksymalnego czasu obsługi incydentów dla poszczególnych priorytetów.

Rejestr incydentów zawierał informacje dot. daty i godziny zgłoszenia incydentu, daty i godziny zamknięcia jego obsługi, opisu podjętych działań naprawczych, imienia i nazwiska pracownika zgłaszającego oraz 2 kategorie priorytetów incydentów (*normalny* i *wysoki*). Prowadzony był w programie nVision uruchomionym w 2017 r.[34], a dodatkowo do końca 2018 r. zdarzenia można było zgłaszać za pomocą konta pocztowego incydent@uokik.gov.pl. Dostęp do programu nVision mają wszyscy pracownicy. Pierwsza kwalifikacja zdarzenia prowadzona jest przez wyznaczonych pracowników Wydziału Informatyki. Jeśli zgłoszenie nie kwalifikuje się do kategorii incydentu jego obsługę zapewnia firma zewnętrzna w ramach umowy cywilnoprawnej. Natomiast zgłoszenia spełniające ww. kryterium rozpatrywane są przez pracowników Wydziału Informatyki. Sposób postępowania ze zdarzeniami nie został jednak uregulowany w regulacjach wewnętrznych. W opinii UOKiK[35], niemalże każda czynność wykonywana przez Urząd wiąże się z przetwarzaniem danych osobowych, stąd *Instrukcja zarządzania systemem informatycznym* reguluje kompleksowo identyfikację, rejestrowanie, analizę, podejmowanie działań naprawczych w większości systemów informatycznych UOKiK.

Nie można zgodzić się, że niemalże każda czynność wykonywana przez Urząd wiąże się z przetwarzaniem danych osobowych. Biorąc pod uwagę zakres działalności UOKiK stwierdzić należy, że Jednostka dysponuje również innymi informacjami i danymi, dla których powinien być zapewniony odpowiedni poziom bezpieczeństwa.

9. [szkolenia] Nadal nie przeszkolono wszystkich pracowników z zakresu bezpieczeństwa informacji, w tym nowych zagrożeń, adekwatnych zabezpieczeń, skutków ewentualnych incydentów naruszenia bezpieczeństwa informacji (szkolenie zorganizowano dla 195 z 512[36], tj. 38% pracowników). Nie wdrożono również zasad dotyczących zapewnienia wiedzy pracownikom w ww. obszarach, w tym wprowadzających cykliczność tych działań.

---

[32] Pismo Za-cy Dyrektora BP z 3 grudnia 2019 r., nr: BP-4.0910.1.2019.

[33] Rozdział IV pkt 2.3 *Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych*, zatwierdzonych przez Ministra Cyfryzacji 15 grudnia 2015 r.

[34] Pierwszy incydent został zaewidencjonowany z datą 23 października 2017 r.

[35] Wyjaśnienia Za-cy Dyrektora BP z 3 grudnia 2019 r., nr: BP-4.0910.1.2019.

[36] Wg stanu zatrudnienia na dzień 7 listopada 2019 r.

Zorganizowano także specjalistyczne szkolenia dla Inspektora ochrony danych osobowych w zw. z wejściem w życie przepisów RODO[37] oraz dla pracowników Wydziału Informatyki[38]. Wyjaśniono[39], że szkolenia z zakresu bezpieczeństwa informacji są *na stałe wpisywane do planu szkoleń*. W 2019 r. szkolenia zewnętrzne jednak nie zostały zorganizowane ze względu na ograniczone zasoby, niemniej Urząd deklaruje, że będą one kontynuowane. Zaplanowano włączenie ww. szkoleń do zakresu służby przygotowawczej. Ponadto w ocenie Jednostki wymóg opracowania zasad dotyczących zapewnienia wiedzy pracownikom został spełniony poprzez zamieszczenie w *Instrukcji Zarządzania Systemem Informatycznym* wśród zadań Administratora Systemu Informatycznego obowiązku zgłaszania zapotrzebowania na szkolenia w przedmiotowym zakresie.

Wskazanie obowiązku złożenia zgłoszenia na szkolenia nie stanowi wypełnienia wymogu opracowania ww. zasad. W szczególności powinny one przedstawiać podejście Jednostki do zarządzania wiedzą w obszarze bezpieczeństwa informacji, zapewnić cykliczność i dostępność do różnych form edukacji dla wszystkich osób zaangażowanych w proces przetwarzania informacji oraz ułatwić tym osobom dostęp do aktualnej wiedzy w ww. zakresie.

10. Zrealizowano obowiązek składania przez pracowników oświadczenia o zapoznaniu się z *Polityką Przetwarzania Danych Osobowych* oraz *Instrukcją Zarządzania Systemem Informatycznym*. Z wdrożonymi regulacjami w 2017 r. zostały zapoznane wszystkie osoby poddane badaniu, natomiast w zakresie zmiany regulacji, oświadczenia złożyło 24 z 25 (96%) poddanych kontroli osób.

Kontroli dot. prawidłowości złożonych oświadczeń poddano 25[40] z 512 (5%) pracowników zatrudnionych na 7 listopada 2019 r. oraz 1 z 6 (17%) pracowników wykonujących pracę w trybie telepracy. Oświadczenia o zapoznaniu się ze zmianą ww. regulacji wprowadzoną w 2018 r. nie złożyła 1 osoba. Oświadczenie to nie zostało podpisane, bowiem informacja o powrocie do pracy osoby z długotrwałej nieobecności nie dotarła do Inspektora Ochrony Danych[41]. Wskazano, że brak zostanie niezwłocznie uzupełniony.

11. [projektowanie i eksploatacja systemów teleinformatycznych] Nie wprowadzono regulacji wewnętrznych w zakresie projektowania, wdrażania oraz wprowadzania zmian w systemach teleinformatycznych, tym samym nie zrealizowano zalecenia pokontrolnego KPRM.

Wyjaśniono[42], że procedura zostanie wdrożona w ramach *SZBI*. Obecnie projektowanie i wdrażanie systemów teleinformatycznych oraz przeprowadzanie zmian w tych systemach regulują zawarte przez Urząd umowy. W uzasadnionych przypadkach powołuje się zespoły, których zadaniem jest wdrożenie przedmiotowych rozwiązań.

12. [SHRIMPv2] Urząd 6 maja 2019 r. podpisał umowę w zakresie realizacji projektu utworzenia Systemu Monitorowania Pomocy Publicznej SHRIMPv2, na wykonanie którego otrzymał dofinansowanie ze środków UE. Zgodnie z przyjętą przez Jednostkę koncepcją nowy system ma być zgodny z wymogami *Rozporządzenia KRI*.

Wdrożenie nowej wersji systemu wynikało z konieczności zapewnienia ciągłej i niezakłóconej pracy zw. z obsługą kilkutysięcznej liczby użytkowników i dostosowania systemu do wymogów *Rozporządzenia KRI*. Z uwagi na przestarzałą technologię dotychczasowy system nie był dostosowany do przetwarzania aktualnej liczby wprowadzanych danych i współdziałania z systemami informatycznymi użytkowników końcowych. Dlatego w latach 2017-2018 dokonano analizy potrzeb i opracowano założenia do nowego systemu. 1 września 2018 r. ogłoszono przetarg, natomiast 6 maja 2019 r. podpisano umowę z wybranym wykonawcą. Zgodnie z wyjaśnieniami[43] nowy system wraz z infrastrukturą techniczną ma zostać odebrany w 2020 r.

13. [SHRIMP] Pozytywnie należy ocenić zgłoszenie Prezesa UOKiK do systemu jako Podmiot Udzielający Pomocy oraz rozdzielenie konta administratora od konta użytkownika merytorycznego,

[37] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
[38] Szkolenia dotyczące bezpieczeństwa teleinformatycznego, sieci komputerowych, aplikacji mobilnych oraz administrowania systemem PAM.
[39] Pismo Za-cy Dyrektora BP z 22 listopada 2019 r., nr: BP-4.0910.1.2019.
[40] Doboru próby dokonano na podstawie *Zestawienia zatrudnionych osób wg stanu na dzień 7 listopada 2019 r.* metodą wyboru losowego, ze stałym odstępem.
[41] Pismo Inspektora Ochrony Danych z 4 grudnia 2019 r., nr: BP-4.0910.1.2019.
[42] Załącznik do pisma Z-cy Dyrektora BP z 15 listopada 2019 r., nr: BP-4.0910.1.2019.
[43] Pismo Za-cy Dyrektora BP z 21 listopada 2019 r., nr: BP-4.0910.1.2019.

dedykowanego wyłącznie sprawozdawczości w zakresie udzielonej pomocy *de minimis* przez kierownika Jednostki. Jednakże z uwagi na ograniczenia funkcjonalne ww. systemu Urząd nie posiadał możliwości utworzenia imiennych kont administratorów, dlatego do poszczególnych kont dodano jedynie dane umożliwiające ich identyfikację. Powyższe rozwiązanie wymaga dalszego dostosowania do pełnego wdrożenia *Rozporządzenia KRI.*

> Prezes UOKiK został zgłoszony do systemu SHRIMP w trybie przewidzianym w § 4 *rozporządzenia w sprawie przekazywania sprawozdań o udzielonej pomocy publicznej i informacji o nieudzieleniu takiej pomocy z wykorzystaniem aplikacji SHRIMP*[44]. Z dniem 13 października 2017 r. obowiązki użytkownika aplikacji odpowiedzialnego za zamieszczanie informacji o udzielonej pomocy *de minimis* przez Prezesa UOKiK powierzono Naczelnikowi Wydziału Sprawozdawczości, a następnie w związku z jego długotrwałą, usprawiedliwioną nieobecnością w pracy, zadania przejął starszy specjalista w ww. Wydziale otrzymując uprawnienia użytkownika podrzędnego[45].

14. W wewnętrznym regulaminie organizacyjnym Departamentu Monitorowania Pomocy Publicznej oraz w opisach stanowisk pracy[46] nie wskazano zadań związanych ze sporządzaniem i wczytywaniem do systemu SHRIMP sprawozdań o pomocy *de minimis* udzielanej przez Prezesa UOKiK.

> Regulacje wewnętrzne nie zostały zmienione z uwagi na niewielką liczbę decyzji o udzieleniu pomocy publicznej wydanych w ostatnich latach[47]. Wskazano, że czas potrzebny na realizację tego zadania to kilka minut i w związku z tym mieści się ono w opisach stanowisk w kategorii innych zadań zleconych przez przełożonych.

W poprzedniej kontroli wyjaśniano, że uprawnienia przyznane użytkownikom w systemach teleinformatycznych powinny wynikać wprost z przydzielonych zadań określonych w opisie stanowiska pracy. Obowiązek wczytywania do systemu SHRIMP sprawozdań o pomocy *de minimis* udzielanej przez Prezesa UOKiK stanowił uzasadnienie do wyodrębnienia indywidualnego konta użytkownika merytorycznego w ww. systemie, zatem powinno ono zostać uwzględnione w opisie stanowiska pracy.

15. [uprawnienia] Mimo stwierdzenia nieprawidłowości w poprzedniej kontroli KPRM w zakresie braku zasad zobowiązujących pracowników UOKiK do dokumentowania nadawania, zmiany i odbierania uprawnień dla użytkowników i administratorów systemów teleinformatycznych nadal nie zostały one wdrożone.

> Obszar zarządzania uprawnieniami został uregulowany w *Instrukcji zarządzania systemem informatycznym*[48]. Jednakże odnosiła się ona tylko do nadawania uprawnień w systemie informatycznym[49], zatem nie dotyczyła działań w zakresie dostępu do systemów teleinformatycznych[50] (odrębnie zdefiniowanych). Wyjaśniono[51], że ww. *Instrukcja* dotyczy systemów teleinformatycznych, ponieważ zawarto w niej postanowienia mówiące o powiązaniu systemu informatycznego z siecią publiczną, a ponadto wskazano, że została opracowana w oparciu o wymogi *Rozporządzenia KRI.* Natomiast w odniesieniu do braku postanowień dot. nadawania, zmiany i odbierania uprawnień dla administratorów systemów wskazano, że formułuje ona generalne zasady modyfikowania uprawnień, zatem nie zastrzega, że nie odnosi się do administratorów systemów informatycznych.

Pojęcia systemu informatycznego i teleinformatycznego nie są tożsame. Zamieszczenie w ww. *Instrukcji* postanowień wskazujących na połączenie systemu informatycznego z siecią publiczną nie wypełnia definicji *systemu teleinformatycznego*. Wskazanie również informacji,

---

[44] Rozporządzenie Rady Ministrów z 23 grudnia 2009 r. w sprawie przekazywania sprawozdań o udzielonej pomocy publicznej i informacji o nieudzieleniu takiej pomocy z wykorzystaniem aplikacji SHRIMP (Dz. U. z 2018 r. poz. 712) obowiązywało do 31 grudnia 2019 r. i zostało zastąpione przez rozporządzenie Rady Ministrów z 23 grudnia 2019 r. w sprawie sposobu udzielania dostępu do aplikacji SHRIMP (Dz. U. poz. 2520).

[45] Zgodnie z instrukcją użytkownika SHRIMP, https://www.uokik.gov.pl/sporzadzanie_sprawozdan_z_wykorzystaniem_aplikacji_shrimp.php#faq1946, dostęp 25 listopada 2019 r.

[46] Opisy stanowisk pracy z 28 lutego 2017 r. Naczelnika Wydziału oraz starszego specjalisty.

[47] Pismo Dyrektora Departamentu Monitorowania Pomocy Publicznej z 2 grudnia 2019 r., nr: DMP-4.071.8.2019.BG.

[48] Pkt 2.1 *Procedury nadawania i rejestrowania uprawnień do przetwarzania danych oraz sposoby uwierzytelnienia.*

[49] Użyta definicja: *Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.*

[50] Użyta definicja: *Zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (…)* [Dz. U. z 2019 r., poz. 2460, t. j. ze zm.].

[51] Pismo Za-cy Dyrektora BP z 25 listopada 2019 r., nr: BP-4.0910.1.2019.

że dokument został opracowany w oparciu o wytyczne zawarte w *Rozporządzeniu KRI* nie powoduje, że jego poszczególne postanowienia odnoszą się do *systemów teleinformatycznych*, tym bardziej, jeśli dalsza treść dokumentu precyzyjnie odnosi się do systemów informatycznych. Ponadto dla zapewnienia bezpieczeństwa informacji konieczne jest jasne określenie zasad nadawania uprawnień i zapewnienie podziału obowiązków dla poszczególnych kategorii użytkowników systemów, w tym administratorów, choćby w celu uniknięcia konfliktu interesów.

> Nadawanie oraz zmiana uprawnień dla pracowników odbywała się na podst. wniosku[52] kierowanego do Wydziału Informatyki. Wniosek dot. wyłącznie zasobów informatycznych i nie był czytelnym dokumentem w zakresie zmiany uprawnień, tj. nie wskazywał, na czym polegać ma zmiana uprawnień i jakie jest jej uzasadnienie. Wyjaśniono[53], że uprawnienia są nadawane na wniosek skierowany przez dyrektora komórki, który jako przełożony określa zakres obowiązków pracownika, a następnie wyznacza zakres danych, do których powinien mieć on dostęp. Zasady te odnoszą się także do zmiany zakresu obowiązków.

Należy podkreślić, że niewdrożenie zasad zarządzania uprawnieniami w systemach teleinformatycznych wpływa na obniżenie poziomu ochrony i bezpieczeństwa informacji.

16. [umowy] Pomimo zalecenia pokontrolnego KPRM nadal postanowienia w umowach na obsługę i utrzymanie systemów teleinformatycznych nie gwarantowały należytego zabezpieczenia interesów UOKiK. Ponadto ze względu na nieustanowienie katalogu niezbędnych postanowień dot. ochrony i bezpieczeństwa informacji, jakie powinny być zamieszczone w umowach, obszar ten nie był wspierany przez regulacje wewnętrzne.

> W okresie od 20 czerwca 2017 r. do 7 listopada 2019 r. zawarto 46 umów na obsługę i utrzymanie systemów teleinformatycznych[54]. Umowy te zostały zawarte na łączną kwotę 8 061 887 zł (brutto). Kontroli poddano 12[55] (z 46, tj. 26%) umów zawartych na łączną kwotę 2 109 741 zł (tj. 26%).
>
> W 9[56] z 12 (tj. 75%) skontrolowanych umowach nie zawarto postanowień dot. bezstronności wykonawców, a w 7[57] (tj. 58%) nie zobowiązano wykonawców do przestrzegania zasad bezpieczeństwa informacji obowiązujących w Urzędzie. Ponadto postanowienia dot. zachowania poufności były bardzo ogólne. W przypadku 8[58] (tj. 67 %) umów nie zobowiązano wykonawców do zachowania w tajemnicy informacji uzyskanych w ramach jej realizacji, również po zakończeniu umowy, w tym w 3[59] przypadkach postanowienia w zakresie poufności sformułowano wyłącznie w odniesieniu do ochrony danych osobowych.
>
> W UOKiK wdrożono *Regulamin w sprawie trybu postępowania w zakresie dokonywania wydatków ze środków publicznych i udzielania zamówień publicznych*[60], nie zawierał jednak on katalogu niezbędnych postanowień dot. ochrony i bezpieczeństwa informacji, jakie powinny być zamieszczone w umowach. Regulacja nie odnosiła się do zasad bezstronności, poufności oraz konieczności zobowiązania wykonawców do przestrzegania standardów bezpieczeństwa informacji obowiązujących w Urzędzie. Istotnym jest, że na konieczność zawierania w umowach postanowień dot. poufności wskazywał również Administrator Bezpieczeństwa Informacji w toku przeprowadzonego *sprawdzenia umów cywilnoprawnych zawieranych z kontrahentami pod kątem zawartości klauzuli poufności*[61].

---

[52] Wniosek o nadanie/odebranie uprawnień do zasobów informatycznych UOKiK, wprowadzonego zarządzeniem Nr 67/2017 DG UOKiK z 7 listopada 2017 r., zmodyfikowanego na mocy zarządzenia Nr 9/2019 Prezesa UOKiK z 12 marca 2019 r.

[53] Pismo Za-cy Dyrektora BP z 25 listopada 2019 r., nr: BP-4.0910.1.2019.

[54] Zgodnie z *Wykazem umów obowiązujących w UOKiK na obsługę i utrzymanie systemów teleinformatycznych w okresie od 20 czerwca 2017 r. do 7 listopada 2019 r.* przekazanym przez UOKiK 28 listopada 2019 r.

[55] Wybór próby nastąpił metodą doboru celowego przy zastosowaniu następujących kryteriów: przedmiot umowy zbieżny z zakresem nieprawidłowości stwierdzonych w toku kontroli KPRM z 2017 r., powtarzalność umów zawieranych w danym zakresie z danym przedsiębiorcą/osobą, istotność przedmiotu umowy ze względu na działalność UOKiK, wysoką wartość całkowitą przedmiotu umowy. Kontroli poddano umowy z: 15 maja 2019 r., nr: BBA-2.0220.30.2019; 1 lutego 2018 r., nr: BBA-2/0221-21/2018; 1 marca 2019 r., nr: BBA-2.0221.34.2019; 28 lutego 2018 r., nr: BBA-2/0221-27/2018/II; 29 grudnia 2017 r., nr: BBA-2/0221-192/2017; 14 czerwca 2019 r., nr: BBA-2.0221.81.2019; 8 sierpnia 2019 r., nr: BBA-2.0221.92.2019; 5 czerwca 2019 r., nr: BBA-2.0221.73.2019; 6 maja 2019 r., nr: BBA-2.0221.65.2019; 31 października 2019 r., nr: BBA-2.0221.113.2019; 30 maja 2018 r., nr: BBA-2/0220-30/2018/I; 31 maja 2019 r., nr: BBA-2.0220.34.2019.

[56] Umowy zawarte: 28 lutego 2018 r., nr: BBA-2/0221-27/2018/II; 31 października 2019 r., nr: BBA-2.0221.113.2019; 30 maja 2018 r., nr: BBA-2/0220-30/2018/I; 31 maja 2019 r., nr: BBA-2.0220.34.2019; 5 czerwca 2019 r., nr: BBA-2.0221.73.2019; 1 lutego 2018 r., nr: BBA-2/0221-21/2018; 29 grudnia 2017 r., nr: BBA-2/0221-192/2017; 14 czerwca 2019 r., nr: BBA-2.0221.81.2019 i 8 sierpnia 2019 r., nr: BBA-2.0221.92.2019.

[57] Umowy zawarte: 31 października 2019 r., nr: BBA-2.0221.113.2019; 30 maja 2018 r., nr: BBA-2/0220-30/2018/I; 31 maja 2019 r., nr: BBA-2.0220.34.2019; 1 lutego 2018 r., nr: BBA-2/0221-21/2018; 29 grudnia 2017 r., nr: BBA-2/0221-192/2017; 14 czerwca 2019 r., nr: BBA-2.0221.81.2019 i 8 sierpnia 2019 r., nr: BBA-2.0221.92.2019.

[58] Umowy zawarte: 28 lutego 2018 r., nr: BBA-2/0221-27/2018/II; 31 października 2019 r., nr: BBA-2.0221.113.2019; 30 maja 2018 r., nr: BBA-2/0220-30/2018/I; 31 maja 2019 r., nr: BBA-2.0220.34.2019; 5 czerwca 2019 r., nr: BBA-2.0221.73.2019; 1 lutego 2018 r., nr: BBA-2/0221-21/2018; 29 grudnia 2017 r., nr: BBA-2/0221-192/2017 i 14 czerwca 2019 r., nr: BBA-2.0221.81.2019.

[59] Umowy zawarte: 28 lutego 2018 r., nr: BBA-2/0221-27/2018/II; 5 czerwca 2019 r., nr: BBA-2.0221.73.2019 i 14 czerwca 2019 r., nr: BBA-2.0221.81.2019.

[60] Zarz. Nr 6/2019 DG UOKiK z 21 stycznia 2019 r. *w sprawie ustalenia regulaminu dokonywania wydatków ze środków publicznych i udzielania zamówień publicznych*.

[61] Sprawozdanie ze sprawdzenia ABI z 7 lutego 2018 r., nr: BKSiO-0142-1(3)/18/JO.

Wyjaśniono[62], że Urząd w trakcie opracowywania *PBI* dokona analizy istniejących w umowach postanowień dot. kwestii poufności z uwzględnieniem charakteru usług świadczonych na rzecz UOKiK, a także informacji i danych udostępnianych podmiotom zewnętrznym realizujących usługi oraz wprowadzi – według potrzeb – stosowne zmiany.

Dla bezpieczeństwa przetwarzanych informacji i należytego zabezpieczenia interesów Jednostki niezbędne jest wskazanie w umowach zasad bezpieczeństwa. Dzięki nim świadczący usługi będą mogli stosować te same standardy i zachowany będzie wymagany poziom bezpieczeństwa. Ułatwi to również dochodzenie praw przez UOKiK w przypadku ewentualnych sporów.

17. Urząd ujednolicił priorytety zgłoszeń dla zdarzeń, które były realizowane w ramach umów dotyczących wsparcia użytkowników sieci komputerowej UOKiK (dalej: umowy helpdesk) z priorytetami obsługiwanymi w aplikacji dedykowanej do obsługi zgłoszeń. Jednakże nadal nie wdrożył zasad pozwalających na rzetelne rozliczenie umów, w oparciu o ich rzeczywisty a nie szacunkowy zakres realizacji. Dokumentacja stanowiąca podstawę odbioru przedmiotu umów helpdesk oraz umowy wspierającej UOKiK w nadzorze nad bezpieczeństwem sieci teleinformatycznej (dalej: umowa wsparcia sieci) nie zawierała informacji o zachowaniu przez wykonawcę poziomu jakości usług określonego w umowach.

W okresie objętym kontrolą obowiązywało 6[63] umów helpdesk na łączną kwotę 767 539 zł oraz umowa[64] wsparcia sieci na kwotę 61 992 zł. Badaniu poddano 3[65] umowy helpdesk o łącznej kwocie 297 202 zł (brutto) oraz ww. umowę wsparcia sieci.

W analizowanych umowach przyjęto realizację zgłoszeń z podziałem na 2 priorytety określone jako *wysoki*[66] i *normalny*[67] oraz ustalono kary umowne za niedotrzymanie standardów jakościowych. Jednakże w przypadku umów helpdesk zarówno protokoły odbioru usług za poszczególne miesiące, jak i przedstawione *Raporty SLA w zamkniętych zgłoszeniach w ujęciu miesięcznym* (dalej: *Raporty SLA*) nie określały liczby zdarzeń załatwionych w terminie i po terminie z podziałem na ww. priorytety. Zatem na ich podstawie nie można było stwierdzić, czy wykonawca dotrzymał umownego poziomu jakości usług w obu priorytetach. Natomiast w przypadku umowy wsparcia sieci odbiór umowy następował na podstawie wykazów przesłanych przez wykonawcę, a Urząd nie dysponował narzędziem umożliwiającym weryfikację prawidłowości wykonania przedmiotu umowy.

Brak pełnych danych zawartych w *Raportach SLA* oraz narzędzi do weryfikacji prawidłowości wykonania przedmiotu umowy wsparcia sieci generował ryzyko odbioru umów, których przedmiot nie został należycie wykonany, tym samym narażał Skarb Państwa na poniesienie nieuzasadnionych wydatków.

18. W przypadku umów na prowadzenie serwera dedykowanego prawidłowy sposób realizacji umowy nie był potwierdzany przez pracownika UOKiK, pomimo że w toku poprzedniej kontroli zwracano uwagę na brak dokumentacji w zakresie odbioru przedmiotu umowy.

W okresie objętym kontrolą zawarto 2[68] umowy na prowadzenie serwera dedykowanego. Za nadzór nad realizacją ww. umów odpowiedzialny był Dyrektor BP[69] albo osoba przez niego wyznaczona. W przypadku pierwszej umowy[70] w aktach znajdowały się m.in. miesięczne raporty z wykonanych usług, przygotowane przez wykonawcę za cały okres obowiązywania umowy. Natomiast w odniesieniu do drugiej umowy[71] przedstawiono jedynie raport za okres 1-31 października 2019 r. Raporty te nie posiadały adnotacji pracownika UOKiK odpowiedzialnego za nadzór nad realizacją umowy, które potwierdzałyby zgodność wykonanej usługi z warunkami umowy. Wyjaśniono[72], że pracownicy weryfikujący poprawność usługi zostali pouczeni o konieczności weryfikowania zgodności wykonanej usługi z warunkami umowy.

---

[62] Pismo Za-cy Dyrektora BP z 18 grudnia 2019 r, nr: BP-4.0910.1.2019.
[63] Umowy zawarte: 28 września 2016 r., nr: DBA-2/243-102-2016; 29 grudnia 2017 r., nr: BBA-2/0221-192/2017; 28 lutego 2018 r., nr: BBA-2/0221-27/2018/I; 7 maja 2018 r., nr: BBA-2/0221-71/2018; 14 czerwca 2019 r., nr: BBA-2.0221.81.2019; 8 sierpnia 2019 r., nr: BBA-2.0221.92.2019.
[64] Umowa zawarta 5 czerwca 2019 r., nr: BBA-2.0221.73.2019.
[65] Umowy zawarte 29 grudnia 2017 r., nr: BBA-2/0221-192/2017; 14 czerwca 2019 r., nr: BBA-2.0221.81.2019 i 8 sierpnia 2019 r. nr: BBA-2.0221.92.2019.
[66] Z gwarantowanym czasem naprawy wynoszącym 4 godziny robocze.
[67] Z gwarantowanym czasem naprawy wynoszącym 8 godzin roboczych.
[68] Umowy zawarte 1 lutego 2018 r., nr: BBA-2/0221-21/2018 i 1 marca 2019 r., nr: BBA-2.0221.34.2019.
[69] Do 14 marca 2018 r. Dyrektor Biura Budżetu i Administracji.
[70] Zawartej 1 lutego 2018 r., nr: BBA-2/0221-21/2018.
[71] Zawartej 1 marca 2019 r., nr: BBA-2.0221.34.2019.
[72] Pismo Za-cy Dyrektora BP z 17 grudnia 2019 r., nr: BP-4.0910.1.2019.

19. [praca na odległość] UOKiK nie wdrożył kompleksowych regulacji dotyczącej zasad bezpiecznej pracy użytkowników przy wykorzystaniu urządzeń przenośnych, jak również pracy na odległość (telepracy). Wprowadzona *Instrukcja zarządzania systemem informatycznym* nie stanowiła skutecznego narzędzia do zarządzania tym obszarem, ponieważ odnosiła się jedynie do komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych. Ponadto nie regulowała wszystkich zagadnień związanych z bezpieczeństwem informacji.

> Na dzień 7 listopada 2019 r. w trybie telepracy pracowało 6 pracowników. W Jednostce obowiązywała *Instrukcja zarządzania systemem informatycznym*, jednakże nie określała ona charakteru zadań, w przypadku których UOKiK dopuszcza możliwość pracy na odległość oraz nie zawierała żadnych regulacji w zakresie wykorzystania systemów teleinformatycznych Urzędu do tego typu pracy, wykorzystania przenośnych nośników danych, opisu zabezpieczeń stosowanych na tego rodzaju urządzeniach, np. mechanizmów szyfrujących zawartość dysków twardych i nośników danych, sposobów i częstotliwości archiwizowania danych, ewentualnej możliwości bądź zakazu korzystania z prywatnego sprzętu do pracy na odległość. Wyjaśniono[73], że zasady wykonywania pracy na odległość zostały uregulowane w rozdziale VI *Regulaminu pracy UOKiK*[74]. Jednakże należy zauważyć, że regulacja ta podlegała już ocenie kontroli KPRM przeprowadzonej w 2017 r., a postanowienia przedmiotowego *Regulaminu* po ww. kontroli nie zostały zmienione. Wskazano również[75], że kompleksowa regulacja zostanie uwzględniona w opracowanym *SZBI*.

Biorąc pod uwagę, że liczba osób wykonujących pracę w trybie telepracy zwiększyła się, zasadnym jest opracowanie i przyjęcie procedur przeciwdziałających zagrożeniom w tym obszarze.

20. [zabezpieczenia techniczno-organizacyjne dostępu do informacji] UOKiK nie posiadał opracowanych zasad dot. ochrony informacji przetwarzanych w systemach teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, które zawierałyby w szczególności wymagania odnośnie sprzętu i oprogramowania, a także regulacji w zakresie utylizacji sprzętu informatycznego. Ponadto zawarte w *Instrukcji zarządzania systemem informatycznym* wytyczne w zakresie naprawy sprzętu odnosiły się wyłącznie do sposobu postępowania z urządzeniami wchodzącymi w skład systemu informatycznego przetwarzającego dane osobowe.

> Wyjaśniono[76], że dotychczasowe prace nad *SZBI* wykazały, że Urząd w pierwszej kolejności będzie potrzebował narzędzia do ochrony informacji przetwarzanych drogą elektroniczną. W związku z tym podjęto decyzję o zakupie oprogramowania zabezpieczającego przed utratą danych, szyfrowania dysków stacji roboczych i laptopów. Ponadto wskazano[77], że unormowania dot. naprawy i utylizacji sprzętu informatycznego zapisano w pkt. 9 *Instrukcji zarządzania systemem informatycznym*. Należy zauważyć, że regulacja ta nie zawierała zasad utylizacji sprzętu informatycznego, natomiast w zakresie naprawy odnosiła się jedynie do urządzeń wchodzących w skład systemu informatycznego przetwarzającego dane osobowe.

UOKiK powinien wdrażać narzędzia zwiększające ochronę informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami oraz opracować pełną dokumentację w tym zakresie, która wspomoże użytkowników w prawidłowej realizacji zadań.

21. Dostęp do pomieszczeń serwerowni możliwy był przy użyciu karty elektromagnetycznej i rejestrowany był w systemie *Kontroli Dostępu*. Urząd nie posiadał jednak dokumentacji potwierdzającej, że dokonywano analizy zapisów odnotowanych w ww. systemie w celu wykrycia nieautoryzowanych działań.

> Każdorazowa próba otworzenia drzwi do serwerowni za pośrednictwem karty elektromagnetycznej jest odnotowywana w programie PControl KDRCP 1.94. Program wskazuje udane próby autoryzacyjne (wejścia do pomieszczenia serwerowni przez uprawnionego pracownika), jak również próby nieautoryzowanych działań. Ponadto w serwerowni głównej prowadzona była także

[73] Pismo Zastępcy Dyrektora BP z 27 listopada 2019 r., znak: BP-4.0910.1.2019.
[74] Zarządzenie Nr 19/2016 Dyrektora Generalnego UOKiK z dnia 16 listopada 2016 r. *w sprawie wprowadzenia w życie Regulaminu pracy UOKiK*, wraz ze zmianami wprowadzonymi zarządzeniami: Nr 40/2017 z dnia 27 czerwca 2017 r., Nr 4/2018 z dnia 16 stycznia 2018 r., Nr 9/2019 z dnia 15 marca 2019 r.
[75] Pismo Zastępcy Dyrektora BP z 17 grudnia 2019 r., znak: BP-4.0910.1.2019.
[76] Załącznik do pisma Za-cy Dyrektora BP z 15 listopada 2019 r., nr: BP-4.0910.1.2019 oraz pismo z 17 grudnia 2019 r., nr: BP-4.0910.1.2019.
[77] Pismo Za-cy Dyrektora BP z 27 listopada 2019 r., nr: BP-4.0910.1.2019.

papierowa *Książka wejść/wyjść*. Wyjaśniono[78], że nie sporządzano notatek z czynności prowadzonych analiz wejść i wyjść do serwerowni. Wskazać również należy, że drzwi do serwerowni zabezpieczone są dodatkowo zamkiem na klucz, który pozostaje w dyspozycji Wydziału Informatyki. Zatem wejście do tych pomieszczeń możliwe jest tylko w obecności upoważnionego pracownika tego Wydziału.

UOKiK powinien dokumentować prowadzone analizy wejść i wyjść z serwerowni, bowiem pozwolą one na ocenę skali nieautoryzowanych działań, a w przypadku licznych zdarzeń w tym zakresie wdrożenie adekwatnych rozwiązań.

22. [zabezpieczenia organizacyjno-techniczne systemów] Działania UOKiK rozpoczęte w lutym 2019 r. w zakresie przeniesienia serwerowni do nowo użytkowanego pomieszczenia były zasadne, ze względu na wyższy standard jego wyposażenia. Niemniej jednak nowe pomieszczenie posiada nadal braki w wyposażeniu.

Urząd w 2019 r. rozpoczął użytkowanie dodatkowego pomieszczenia, w którym zlokalizowano tzw. główną serwerownię i sukcesywnie przenosił do niej urządzenia systemowe z dotychczas wykorzystywanej. Wyjaśniono[79], że w związku z przenoszeniem urządzeń systemowych do serwerowni głównej, inwestowanie w podwyższenie standardu serwerowni likwidowanej ze względów ekonomicznych stało się nieracjonalne. Natomiast wyposażenie i modernizacja serwerowni głównej uzależnione będzie od możliwości budżetowych Urzędu.

Pomieszczenie serwerowni stanowi kluczowe miejsce w zakresie bezpieczeństwa informacji, dlatego UOKiK powinien kontynuować czynności związane z poprawą stanu jego wyposażenia.

23. Urząd po kontroli KPRM z 2017 r. wyeliminował zagrożenie bezpieczeństwa informacji gromadzonych w systemach w zakresie wykorzystywania oprogramowania, dla którego producent nie zapewniał wsparcia w postaci poprawek bezpieczeństwa. Komputery z tym oprogramowaniem były wykorzystywane jedynie w laboratoriach i nie zostały podłączone do sieci wewnętrznej.

UOKiK po kontroli KPRM wykorzystywał 7 komputerów z ww. oprogramowaniem, jedynie w laboratoriach do obsługi urządzeń laboratoryjnych. Wyjaśniono[80], że ich wymiana na nowszy sprzęt wiązałaby się z koniecznością zakupu i wymiany oprogramowania urządzeń laboratoryjnych, a czasem całego urządzenia i w związku z tym, ze względów ekonomicznych, w najbliższym czasie nie są planowane zmiany w tym zakresie. Komputery te nie stanowią zagrożenia dla sieci Urzędu, ponieważ nie są do niej podłączone.

24. Obowiązująca *Instrukcja Zarządzania Systemem Informatycznym*[81] nie wskazywała pracowników Urzędu odpowiedzialnych za realizację działań w przypadku ujawnienia złośliwego oprogramowania. Ponadto konieczność podejmowania ww. działań nie została uwzględniona w zakresach obowiązków i opisach stanowisk pracy osób, którym przydzielono takie zadania. Tym samym nadal nie wyeliminowano nieprawidłowości stwierdzonej w poprzedniej kontroli.

Do podejmowania działań w sytuacji ujawnienia wirusa wyznaczono 2 pracowników. Zlecenie wykonywania tych obowiązków nastąpiło w formie ustnej przez bezpośredniego przełożonego[82].

W celu zapewnienia skuteczności podejmowanych działań w przypadku ujawnienia wirusa niezbędne jest wskazanie zadań w tym zakresie i odpowiedzialności za ich realizację w opisach stanowisk wyznaczonych osób.

25. [kopie zapasowe] Od 2019 r. UOKiK wykonuje i testuje kopie zapasowe, a także prowadzi testowanie aktualizacji systemów i oprogramowania na dedykowanym do tego celu środowisku testowym. Jednakże konieczne jest opracowanie procedur wewnętrznych w zakresie regularności ich testowania oraz zasad niszczenia kopii zapasowych i archiwalnych. Ponadto pomimo wdrożenia we wrześniu 2018 r. systemu Elektronicznego Zarządzania Dokumentami (EZD) w *Instrukcji*

[78] Pismo Za-cy Dyrektora BP z 2 grudnia 2019 r., nr: BP-4.0910.1.2019.
[79] Pismo Za-cy Dyrektora BP z 2 grudnia 2019 r., nr: BP-4.0910.1.2019.
[80] Pisma Za-cy Dyrektora BP z 27 listopada 2019 r. i 17 grudnia 2019 r., nr: BP-4.0910.1.2019.
[81] Zarządzeniem wprowadzającym *Instrukcję Zarządzania Systemem Informatycznym uchylono obowiązującą* w toku kontroli KPRM procedurę ochrony antywirusowej i działań podejmowanych po stwierdzeniu wirusa.
[82] Pisma Za-cy Dyrektora BP z 27 listopada 2019 r. i 18 grudnia 2019 r. nr: BP-4.0910.1.2019.

zarządzania systemem informatycznym UOKiK nie wprowadzono postanowień w zakresie konieczności sporządzania kopii zapasowych ww. systemu.

> Wyjaśniono[83], że UOKiK zakupił specjalistyczne maszyny i urządzenia do wirtualizacji, które umożliwiają tworzenie platformy testowej w środowisku wirtualnym. Natomiast wprowadzenie procedury dot. regularności testowania kopii zapasowych, zasady niszczenia kopii zapasowych i archiwalnych oraz nowelizacja właściwych dokumentów w zw. z wprowadzeniem EZD nastąpi w ramach *SZBI*.

Jednostka zobowiązana jest do zapewnienia aktualizacji regulacji wewnętrznych wraz ze zmieniającym się otoczeniem. Zatem regulacje w zakresie konieczności sporządzania kopii zapasowych EZD powinny zostać wdrożone wraz z systemem w 2018 r. Jest to istotne w celu skutecznego zapobiegania utracie przetwarzanych informacji.

26. [plan ciągłości działania] UOKiK nie podjął działań w zakresie opracowania planu ciągłości działania na wypadek wystąpienia zdarzeń o niskim prawdopodobieństwie, ale o katastrofalnych skutkach, takich jak np. pożar, katastrofa budowlana, terroryzm, powódź.

> *W Urzędzie* wdrożono system backupu (AVAMAR) dot. tworzenia kopii zapasowych, który umożliwia odtworzenie kluczowych danych z rejestrów i systemów[84]. W opinii Kontrolowanego[85], UOKiK nie jest zobligowany bezpośrednio do stworzenia planu ciągłości działania, niemniej dostrzega niewątpliwie korzyści płynące z jego posiadania. Jednakże ze względów ekonomicznych jego opracowanie i wdrożenie w pełnym zakresie nie jest obecnie możliwe.

Zgodnie z *Rozporządzeniem KRI*[86] wymagania w zakresie *SZBI* uznaje się za spełnione, jeżeli system ten został opracowany na podstawie Polskich Norm, w tym m.in. normy PN-ISO/IEC 24762, zgodnie z którą zaleca się, by organizacja dysponowała opracowanym planem zachowania ciągłości działania, który będzie już przetestowany oraz utrzymywała go i aktualizowała. Tworzenie kopii zapasowych jest jedynie elementem zapewniającym ciągłość działania. Zatem UOKiK budując spójny *SZBI* powinien kierować się postanowieniami ww. normy i podjąć niezbędne czynności w celu opracowania ww. planu.

27. [rozliczalność] Urząd nie wyeliminował nieprawidłowości dotyczącej zapewnienia rozliczalności działań prowadzonych w systemach teleinformatycznych. Nie posiadał opracowanych procedur w tym przedmiocie, w szczególności określających zasady prowadzenia i wykorzystania dzienników systemowych (logów), w których odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych. Ponadto informacje zawarte w dziennikach systemowych nie były regularnie przeglądane w celu wykrycia nieuprawnionego dostępu lub działań niepożądanych.

> Wyjaśniono[87], że zawartość dzienników analizowana jest w przypadkach awarii systemu, w celu określenia jej przyczyny. W latach 2018-2019 planowano zakup oprogramowania SIEM, który analizuje automatycznie logi i wskazuje przypadki istotne dla bezpieczeństwa. Jednakże z perspektywy jednostki ważniejsze było wdrożenie systemu zabezpieczającego przed wyciekiem danych wrażliwych, dlatego zakup ww. oprogramowania przeniesiono na 2020 r. i uwzględniono w *Planie zamówień publicznych*. Regulacje i procedury powstaną po wdrożeniu oprogramowania SIEM, bowiem po szkoleniach i zapoznaniu się z jego funkcjonalnościami możliwe będzie napisanie stosownych procedur.

Bezpieczeństwo informacji przetwarzanych w systemach wymaga zapewnienia rozliczalności działań w nich podejmowanych, bowiem to ona pozwala przypisać określone działania do konkretnej osoby lub procesu oraz umiejscowić je w czasie. Ważne jest opracowanie zasad w tym przedmiocie oraz regularne przeglądanie informacji zawartych w dziennikach systemowych. Brak specjalistycznego oprogramowania do analizy logów nie może stanowić uzasadnienia

---

[83] Załącznik do pisma z 15 listopada 2019 r., nr: BP-4.0910.1.2019 oraz pismo Za-cy Dyrektora BP z 18 grudnia 2019 r., nr: BP-4.0910.1.2019.
[84] Informacje zawarte w tabeli dot. stopnia wyeliminowania nieprawidłowości – załącznik do pisma z 15 listopada 2019 r., nr: BP-4.0910.1.2019, pkt 29.
[85] Wyjaśnienia Za-cy Dyrektora BP z 18 grudnia 2019 r., nr: BP-4.0910.1.2019.
[86] § 20 ust. 3 ww. Rozporządzenia.
[87] Pismo Za-cy Dyrektora BP z 22 listopada 2019 r., nr: BP-4.0910.1.2019 oraz z 18 grudnia 2019 r., nr: BP-4.0910.1.2019.

do braku regulacji w tym zakresie, bowiem wraz z jego wdrażaniem mogą zostać one zmodyfikowane w odniesieniu do indywidualnych funkcjonalności oprogramowania.

II. Zapewnienie dostępności informacji zawartych na stronie internetowej

28. Pozytywnie należy ocenić, że Urząd dostosował stronę internetową do wymagań określonych w § 19 *Rozporządzenia KRI*, zatem zapewnił jej dostępność dla osób z niepełnosprawnościami.

> Wprowadzone zostały zmiany w zakresie kodu strony internetowej, a także dodano prawidłowe atrybuty oraz identyfikatory dla znaczników HTML. Zastosowanie tych modyfikacji pozwoliło wyeliminować błędy, wskazywane przez zewnętrzne narzędzia służące do przeprowadzenia audytu. Urząd posiadał wyniki testów narzędzia o nazwie *Tingtun Checker*, które nie wykrywało błędów w zakresie dot. wymagań WCAG 2.0. Zapewniono także możliwość zwiększenia wielkości tekstu i nagłówków za pomocą narzędzi przeglądarki. Ponadto nagrania multimedialne zamieszczane były na stronie internetowej obok głównej treści komunikatu prasowego, stanowiły więc alternatywę do głównego tekstu.

III. Wymiana informacji w postaci elektronicznej

29. UOKiK nie zastosował się do ustaleń poprzedniej kontroli i nadal nie opracował procedur określających deklarowany poziom dostępności dostarczanych usług przez systemy teleinformatyczne, o których mowa w § 15 ust. 2 *Rozporządzenia KRI*.

> Wyjaśniono[88], że Urząd zamierza wdrożyć procedury określające poziom dostępności usług realizowanych przez systemy teleinformatyczne w ramach *SZBI*.

Posiadanie ustalonych i udokumentowanych procedur w tym zakresie zapewnia weryfikację sposobu zarządzania usługami, w tym zwłaszcza daje możliwość zidentyfikowania właściciela merytorycznego usług[89], ustalenie odpowiedzialności za utrzymanie usług od strony technicznej oraz określenie i monitorowanie poziomu ich świadczenia.

Biorąc pod uwagę ustalenia i oceny przedstawione w *Wystąpieniu*, zalecam Panu Prezesowi:

1. Pilne zintensyfikowanie działań w celu skutecznej i pełnej realizacji wszystkich zaleceń pokontrolnych wydanych w czerwcu 2017 r., ze szczególnym uwzględnieniem niezwłocznego opracowania pełnej dokumentacji systemu zarządzania bezpieczeństwem informacji.
2. Wprowadzenie narzędzi i mechanizmów zarządczych zapewniających Kierownictwu UOKiK efektywny nadzór nad podejmowanymi działaniami w zakresie bezpieczeństwa informacji oraz wykonaniem zaleceń pokontrolnych KPRM.
3. Okresową ewaluację wdrażania kompleksowego i spójnego systemu zarządzania bezpieczeństwem informacji.

Proszę Pana Prezesa 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 pokontrolnego* nie przysługują środki odwoławcze.

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

Z poważaniem

Michał Dworczyk

Minister-Członek Rady Ministrów

/-podpisano kwalifikowanym podpisem elektronicznym-/

[88] Pismo Za-cy Dyrektora BP z 27 listopada 2019 r. oraz z 18 grudnia 2019 r., nr: BP-4.0910.1.2019.
[89] Komórki organizacyjnej jednostki.