Egz. nr 4

# PEŁNOMOCNIK
# DO SPRAW KONTROLI PRZETWARZANIA
# PRZEZ CENTRALNE BIURO ANTYKORUPCYJNE
# DANYCH OSOBOWYCH

# SPRAWOZDANIE

Warszawa, 19 marca 2014 r.

## WSTĘP

Sprawozdanie przedkładane jest zgodnie z dyspozycją art. 22b ust. 8 *ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (Dz. U. z 2012 r. poz. 621 z późn. zm.; dalej: *ustawa o CBA*), zgodnie z którym pełnomocnik do spraw kontroli przetwarzania przez CBA danych osobowych (dalej: Pełnomocnik) corocznie do dnia 31 marca przedstawia Prezesowi Rady Ministrów, Sejmowej Komisji do Spraw Służb Specjalnych oraz Generalnemu Inspektorowi Ochrony Danych Osobowych – za pośrednictwem Szefa CBA - sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych w CBA oraz wszystkie przypadki naruszeń przepisów w tym zakresie.

Niniejsze *Sprawozdanie* obejmuje okres od 1 stycznia 2013 r. do 31 grudnia 2013 r.

## I. PRAWNO-ORGANIZACYJNA STRUKTURA OCHRONY DANYCH OSOBOWYCH W CBA

W granicach ustawowych zadań, zgodnie z art. 22a ust. 1 *ustawy o CBA,* Centralne Biuro Antykorupcyjne może przetwarzać dane osobowe, w tym dane wskazane w art. 27 ust. 1 *ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*[1], bez wiedzy i zgody osoby, której te dane dotyczą. W celu prawidłowej realizacji tego uprawnienia, a w szczególności dla zapewnienia przestrzegania poniżej wymienionych zasad:

1) legalności – dane mogą być przetwarzane tylko na podstawie przepisów prawa,
2) celowości – dane powinny być zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu, jeśli jest to niezgodne z tymi celami,
3) merytorycznej poprawności – dane powinny być merytorycznie poprawne,
4) adekwatności – dane powinny być adekwatne w stosunku do celów, w jakich są przetwarzane,
5) ograniczenia czasowego – dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie mogą być przetwarzane dłużej, niż jest to niezbędne do osiągnięcia celu, dla którego zostały zebrane,

*decyzją nr 2/11 Szefa CBA z dnia 3 stycznia 2011 r.*[2] został wprowadzony system ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym. System ochrony danych osobowych w CBA tworzą:

- administrator danych osobowych – Szef CBA;
- administrator bezpieczeństwa informacji – jego obowiązki wykonuje Pełnomocnik, a można je najkrócej scharakteryzować jako ciągły nadzór oraz kontrola zasad przetwarzania danych;
- Pełnomocnik – wykonuje przede wszystkim obowiązki, które nałożyła na niego *ustawa o CBA*, głównie kontrolę prawidłowości przetwarzania przez CBA danych osobowych, w szczególności ich przechowywania, weryfikacji i usuwania;
- lokalni administratorzy danych osobowych – kierownicy jednostek organizacyjnych CBA, których zadaniem jest przede wszystkim realizacja obowiązków związanych z ochroną danych osobowych w ramach jednostek organizacyjnych we współpracy z administratorem bezpieczeństwa informacji;
- administrator systemu – kierownik jednostki organizacyjnej CBA, do którego zadań należy zapewnienie ciągłości działania systemów i sieci teleinformatycznych służących do przetwarzania danych osobowych;

---

[1] Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.

[2] *Decyzja nr 2/11 Szefa Centralnego Biura Antykorupcyjnego z dnia 3 stycznia 2011 r. w sprawie systemu ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym* (Dz. Urz. CBA Nr 1, poz. 23).

- administratorzy bezpieczeństwa zbiorów – osoby wyznaczone do nadzorowania przestrzegania i wdrażania dokumentacji przetwarzania danych osobowych w odniesieniu do konkretnych zbiorów.

Załącznikami do wyżej wymienionej decyzji są dwa dokumenty opisujące sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzania danych osobowych w CBA odpowiednią do zagrożeń oraz kategorii danych objętych ochroną:

- *Polityka bezpieczeństwa ochrony danych osobowych w Centralnym Biurze Antykorupcyjnym,*
- *Instrukcja zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w Centralnym Biurze Antykorupcyjnym*[3].

W ramach opisywanego systemu ochrony danych osobowych w CBA przyjęto rozwiązanie, w którym lokalni administratorzy danych osobowych (tj. kierownicy jednostek organizacyjnych Biura) nadają upoważnienia do przetwarzania danych osobowych podległym funkcjonariuszom i pracownikom CBA. Zakres i formę upoważnień określają przepisy dotyczące zakresów obowiązków i odpowiedzialności funkcjonariuszy i pracowników CBA, zgodnie z którymi osoby upoważnione do przetwarzania danych osobowych mogą przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie w upoważnieniu i tylko w celu wykonywania nałożonych na nie obowiązków służbowych. Powyższe rozwiązanie nie narusza wymogu innych form upoważnienia określonych odrębnymi procedurami, zwłaszcza regulującymi dostęp do baz zewnętrznych.

Pełnomocnik prowadzi wewnętrzny wykaz zbiorów danych osobowych przetwarzanych w CBA, w ramach którego wyodrębniono 13 głównych zbiorów danych osobowych, podzielonych funkcjonalnie na podzbiory ze względu na strukturę organizacyjną i zadania wykonywane przez poszczególne jednostki organizacyjne CBA. Opracowany wykaz jest elastyczny, gdyż podlega ciągłej aktualizacji w wyniku kolejnych zgłoszeń dokonywanych przez jednostki organizacyjne Biura. Weryfikacja tych zgłoszeń nie wykazała istnienia jakichkolwiek baz utworzonych bez podstawy prawnej. Prowadzone zbiory odpowiadają zasadzie celowości i adekwatności. Ponadto warto zauważyć, że zakończenie importowania danych kadrowo-płacowych do systemu teleinformatycznego klasy ERP – Narzędzia Informatycznego Wspierania Administracji (NIWA), wyznaczyło w 2013 r. początek procesu sukcesywnego usuwania poszczególnych baz, których zakres danych został skonsumowany przez system. Celem tego procesu jest przeciwdziałanie nieuzasadnionemu powielaniu i rozproszeniu danych osobowych.

Centralne Biuro Antykorupcyjne przetwarza dane wrażliwe, o których mowa w art. 27 ust. 1 *ustawy o ochronie danych osobowych*, a dane te są rozproszone w zbiorach zgłaszanych do wykazu zbiorów CBA. Ich przetwarzanie odbywa się w zakresie niezbędnym i adekwatnym do realizowanych zadań. CBA nie prowadzi baz danych utworzonych wyłącznie w celu gromadzenia danych sensytywnych.

Kolejnym obowiązkiem administratora bezpieczeństwa informacji, związanym z prowadzeniem wykazu zbiorów, jest realizacja procedury zgłaszania Generalnemu Inspektorowi Ochrony Danych Osobowych zbiorów danych przetwarzanych w CBA w przypadkach określonych przepisami. W okresie sprawozdawczym Biuro nie prowadziło zbiorów danych podlegających rejestracji GIODO.

---

[3] Dokumentacja wymagana *rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz. U. Nr 100, poz. 1024), dalej: *rozporządzenie MSWiA z 29.04.2004 r.*

Opisane powyżej struktura i organizacja przetwarzania danych osobowych tworzą spójny i kompleksowy system ochrony danych osobowych w CBA.

## II. PRZESTRZEGANIE PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

### 1. Kontrola

Przetwarzanie danych osobowych przez jednostki organizacyjne Biura w ramach realizacji ich regulaminowych zadań podlega kontroli Pełnomocnika w zakresie prawidłowości ich przetwarzania, w szczególności przechowywania, weryfikacji i usuwania danych zbędnych. W okresie sprawozdawczym nie zaistniały w CBA podstawy do wszczęcia procedury w oparciu o art. 22b ust. 6 *ustawy o CBA,* co oznacza również, że Pełnomocnik nie wydawał poleceń usunięcia stwierdzonych uchybień w tym trybie. Wszystkie kontrole, przeprowadzone przez niego w 2013 roku, zostały wszczęte na podstawie *decyzji nr 3/11 Szefa CBA z dnia 3 stycznia 2011 r. w sprawie określenia zasad i trybu kontroli przetwarzania danych osobowych w Centralnym Biurze Antykorupcyjnym*[4], która reguluje ich planowanie, rodzaje czynności kontrolnych, tryby (kontrola planowa, doraźna i sprawdzająca), sposób dokumentowania ustaleń poczynionych w toku kontroli oraz procedurę odwoławczą (zastrzeżenia do protokołu kontroli).

Powyżej wskazane kontrole nie były prowadzone w trybie kontroli doraźnych, ponieważ w 2013 roku nie zaistniały podstawy do bieżącej potrzeby sprawdzenia prawidłowości przetwarzania danych osobowych. Były one organizowane w oparciu o roczny plan kontroli, z którym zapoznawany jest Szef CBA. I tak z pięciu zaplanowanych kontroli Pełnomocnik przeprowadził cztery kontrole kompleksowe w: Zespole Audytu Wewnętrznego, Biurze Techniki Operacyjnej, Gabinecie Szefa i Biurze Kontroli i Spraw Wewnętrznych. Kontrola w Delegaturze CBA w Szczecinie, z uwagi na zmianę jej siedziby, a także trwającą w tym samym czasie kontrolę ochrony informacji niejawnych, prowadzoną przez Agencję Bezpieczeństwa Wewnętrznego, została przełożona na rok 2014. Kontrole polegały na sprawdzeniu, czy stan faktyczny dotyczący przetwarzania danych osobowych w jednostkach organizacyjnych CBA jest zgodny z przepisami *ustawy o CBA*, przepisami innych aktów powszechnie obowiązujących oraz wewnętrznych regulacji CBA dotyczących ochrony tych danych. W przypadku stwierdzenia rozbieżności obejmowały również ustalenie ich przyczyn i sformułowanie zaleceń dotyczących podjęcia działań w celu usunięcia nieprawidłowości, a także wprowadzenia nowych rozwiązań zmniejszających ryzyko niewłaściwego postępowania z danymi osobowymi.

Programy kontroli obejmowały sprawdzenie:

1) organizacji przetwarzania danych, ze szczególnym uwzględnieniem obowiązku:
   - posiadania upoważnień przez funkcjonariuszy i pracowników do przetwarzania danych osobowych,
   - prowadzenia ewidencji osób upoważnionych przez lokalnego administratora danych osobowych na podstawie upoważnienia Szefa CBA,
   - zapoznania funkcjonariuszy i pracowników z treścią *decyzji nr 2/11* oraz ich przeszkolenia w zakresie ochrony danych osobowych,
   - aktualizacji informacji o zbiorach danych osobowych przetwarzanych przez jednostkę organizacyjną CBA, zgłoszonych do wykazu zbiorów danych osobowych prowadzonego przez Pełnomocnika;
2) prawidłowości przetwarzania danych osobowych w odniesieniu do:
   - podstaw prawnych przetwarzania danych,
   - zgodnego z prawem celu przetwarzania danych,

[4] Dz. Urz. CBA Nr 1, poz. 24.

- adekwatności zakresu danych do celu ich przetwarzania,
- merytorycznej poprawności przetwarzanych danych,
- stosowania przepisów dotyczących archiwizacji i brakowania danych, których dalsze przetwarzanie w jednostce organizacyjnej CBA nie znajduje uzasadnienia,
- prawidłowości sposobu przeprowadzenia weryfikacji materiałów zawierających dane osobowe, w celu ustalenia, czy zawierają dane zbędne lub dane, o których mowa w art. 22a ust. 10 *ustawy o CBA,*
- respektowania zasady ograniczenia czasowego w stosunku do danych tzw. zbędnych, podlegających usunięciu;

3) stanu zabezpieczenia systemów teleinformatycznych służących do przetwarzania danych osobowych, dotyczącego m.in.:
   - wymogów, jakie zgodnie z *rozporządzeniem MSWiA z 29.04.2004 r.* muszą spełniać systemy teleinformatyczne przetwarzające dane jawne,
   - wymogów bezpieczeństwa teleinformatycznego zapisanych w dokumentacji bezpieczeństwa systemów przetwarzających informacje niejawne[5], akredytowanych przez Agencję Bezpieczeństwa Wewnętrznego,
   - obowiązku ewidencjonowania i szyfrowania nośników, na których przetwarzane są dane osobowe (jawne i niejawne),
   - występowania plików multimedialnych niezwiązanych z realizacją zadań służbowych;
4) stanu zabezpieczenia fizycznego przetwarzanych danych osobowych.

**Tabela 1.** Wyniki kontroli przetwarzania danych osobowych za rok 2013.

| Jednostka | Organizacja przetwarzania danych | Prawidłowość przetwarzania danych | Stan zabezpieczenia systemów teleinformatycznych | Stan zabezpieczenia fizycznego | Ocena |
|---|---|---|---|---|---|
| **ZAW** | **bez zastrzeżeń z drobnymi uchybieniami** dotyczącymi aktualizacji wykazu zbiorów | **bez zastrzeżeń** | **bez zastrzeżeń** | **bez zastrzeżeń** | **5** |
| **BKSW** | **bez zastrzeżeń z uchybieniami** dotyczącymi aktualizacji wykazu zbiorów oraz drobnych zmian w ewidencji osób upoważnionych | **bez zastrzeżeń z uchybieniami** dotyczącymi przetwarzania danych w podzbiorze *Urlopy i absencje* oraz zintensyfikowania procesu archiwizacji w odniesieniu do kilkunastu zakończonych spraw | **bez zastrzeżeń z drobnymi uchybieniami** dotyczącymi opisu struktury zbiorów i sposobu wykonywania kopii zapasowych | **bez zastrzeżeń** | **- 5** |
| **GSz** | **bez zastrzeżeń z uchybieniami** dotyczącymi aktualizacji wykazu zbiorów oraz zmian w ewidencji osób upoważnionych | **bez zastrzeżeń z uchybieniami** dotyczącymi przeredagowania klauzuli zgody na przetwarzanie danych. | **bez zastrzeżeń** | **bez zastrzeżeń** | **- 5** |

[5] Procedury Bezpiecznej Eksploatacji oraz Szczególne Wymagania Bezpieczeństwa Systemu.

| | | | | | |
|---|---|---|---|---|---|
| **BTO** | **zastrzeżenia dotyczące nieprawidłowości w zakresie przepisów wewnętrznych** obejmujących: obowiązek zapoznania się z *decyzją nr 2/11*, brak szkolenia w zakresie ochrony danych osobowych, zmiany w ewidencji osób upoważnionych, aktualizację wykazu zbiorów | **bez zastrzeżeń z uchybieniami** dotyczącymi: przetwarzania danych w podzbiorze *Urlopy i absencje* | **bez zastrzeżeń z uchybieniami** dotyczącymi opisu struktury zbiorów i sposobu wykonywania kopii zapasowych | **bez zastrzeżeń** | **4** |

Analiza materiałów z przeprowadzonych kontroli wykazała, że w scharakteryzowanych w tabeli jednostkach organizacyjnych CBA:

- nie stwierdzono przypadków naruszeń przepisów rangi ustawowej;
- stwierdzone uchybienia i nieprawidłowości rozpatrywano w odniesieniu do przepisów wewnętrznych CBA, zaś ich charakter oraz natężenie nie miały zasadniczego wpływu na poziom bezpieczeństwa przetwarzania danych;
- przetwarzanie danych odbywało się z zachowaniem zasad: legalności, celowości, merytorycznej poprawności, adekwatności i ograniczenia czasowego, a drobne w tym zakresie nieścisłości najczęściej wynikały z niewłaściwej interpretacji przepisów.

Dodatkowo Pełnomocnik w ramach nadzoru nad prawidłowością przetwarzania danych osobowych może prowadzić czynności wyjaśniające dotyczące podejrzenia naruszenia przepisów w zakresie nieprawidłowego zabezpieczenia danych osobowych. W 2013 r. nie zarejestrowano w *„Repertorium spraw dotyczących naruszeń przepisów o ochronie danych osobowych"* żadnego zgłoszenia, które stałoby się podstawą do wszczęcia czynności wyjaśniających.

Mając na uwadze powyższe informacje, można wskazać, że – co do zasady – w 2013 roku przetwarzanie danych osobowych w CBA odbywało się zgodnie z obowiązującymi przepisami, z wykorzystaniem środków organizacyjno-prawnych i technicznych gwarantujących im odpowiednią ochronę. Powyższy wniosek uzasadniają wysokie oceny poziomu ochrony danych osobowych w wybranych jednostkach organizacyjnych, będące konsekwencją znikomej skali i niewielkiego ciężaru gatunkowego stwierdzonych w ramach kontroli uchybień i nieprawidłowości.

## 2. Weryfikacja i usuwanie zbędnych danych osobowych

W systemie ochrony danych osobowych w CBA realizowany jest obowiązek weryfikacji niezbędności posiadanych danych, wynikający z art. 22a ust. 8 i 10 *ustawy o CBA*. Jej następstwem jest usunięcie danych, których dalsze przetwarzanie byłoby niezgodne z jego celem. Procedura weryfikacji usuwania danych osobowych w jednostkach organizacyjnych CBA została określona w *decyzji nr 88/11 Szefa Centralnego Biura Antykorupcyjnego z dnia 21 lutego 2011 r. w sprawie określenia trybu weryfikacji i usuwania danych osobowych przetwarzanych w Centralnym Biurze Antykorupcyjnym*[6]. Jej realizacja może odbywać się w trzech formach:

[6] Dz. Urz. CBA Nr 1, poz. 32.

- weryfikacji bieżącej – przeprowadzanej przez funkcjonariusza w trakcie wykonywania zadań służbowych,
- weryfikacji okresowej – do przeprowadzenia której zobligowana jest jednostka organizacyjna nie rzadziej niż raz na 5 lat i którą nadzoruje jej kierownik,
- weryfikacji specjalnej – przeprowadzana w trakcie kontroli lub na podstawie przepisów szczególnych, wymagających zastosowania odrębnego trybu (m.in. art. 22a ust. 10 *ustawy o CBA* dotyczący danych osób podejrzanych o popełnienie przestępstwa, które nie zostały za nie skazane).

Sposób przeprowadzenia weryfikacji był poddany sprawdzeniu w trakcie opisanych wyżej kontroli planowych, w wyniku których nie wykazano nieprawidłowości w tym zakresie. Warto jeszcze raz podkreślić, że nadzór nad weryfikacją i usuwaniem zbędnych danych osobowych jest traktowany jako priorytetowe zadanie Pełnomocnika i stanowi główny obszar zakresu przedmiotowego prowadzonych przez niego kontroli.

## 3. Przedsięwzięcia w zakresie doskonalenia ochrony danych osobowych

W celu podwyższenia poziomu kultury przetwarzania danych osobowych wśród funkcjonariuszy i pracowników CBA wskazaną wcześniej *decyzją nr 2/11 Szefa CBA* został wprowadzony obowiązek uczestniczenia w szkoleniu w zakresie ochrony danych osobowych osób upoważnionych do przetwarzania danych osobowych, a wykonanie tego wymogu jest sprawdzane w ramach prowadzonych kontroli. W 2013 r. przeprowadzono 21 szkoleń obejmujących tematykę ochrony danych osobowych. Szkolenia te realizowane były jako odrębne szkolenia dla osób nowo przyjętych albo powracających do służby/pracy po długiej nieobecności, a które wcześniej nie uczestniczyły w przedmiotowym szkoleniu, jak również jako blok szkoleniowy w ramach odbywających się w CBA szkoleń podstawowych i specjalistycznych.

Program szkoleniowy obejmuje:
- przepisy dotyczące ochrony danych osobowych,
- sposoby ochrony danych przed osobami postronnymi i zasady udostępniania danych osobom, których one dotyczą,
- obowiązki osób upoważnionych do przetwarzania danych osobowych i innych,
- odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych.

W CBA realizowane są również inne szkolenia obejmujące tematykę ochrony danych osobowych, w tym w zakresie bezpieczeństwa i ochrony danych SIS i VIS (w 2013 roku przeprowadzono jedno takie szkolenie).

Warto też wspomnieć, że funkcjonariusze, realizujący z upoważnienia Pełnomocnika jego zadania, w 2013 roku podnosili swoje kwalifikacje uczestnicząc w przygotowanych specjalnie dla nich szkoleniach odbywających się w formie warsztatów, których głównym celem było ugruntowanie posiadanej wiedzy, wyjaśnianie wątpliwości w zakresie przepisów dotyczących ochrony danych osobowych oraz nabycie praktycznych umiejętności prowadzenia kontroli. Uczestniczyli oni również w szkoleniach z zakresu bezpieczeństwa teleinformatycznego, audytu teleinformatycznego oraz metodyki szkolenia dorosłych.

Istotny element działalności informacyjnej i edukacyjnej Pełnomocnika stanowi jego udział w opiniowaniu wewnętrznych i zewnętrznych aktów prawnych dotyczących ochrony danych osobowych. W ramach współpracy z jednostkami organizacyjnymi CBA udziela on również odpowiedzi na pytania dotyczące prawidłowości przetwarzania danych osobowych w każdym aspekcie ustawowej działalności Biura.

W 2013 roku Pełnomocnik opracował algorytm realizacji obowiązku niszczenia określonych danych sensytywnych osób podejrzanych o popełnienie przestępstw, które nie zostały za te przestępstwa skazane, wynikającego z art. 22a ust. 10 *ustawy o CBA*. Wytyczne w tej

sprawie zostały przekazane do stosowania przez wszystkie jednostki organizacyjne CBA przetwarzające tego rodzaju dane osobowe. Algorytm opiera się na wypracowaniu praktyki uzyskiwania przez Biuro informacji o orzeczeniach kończących postępowania karne, w których CBA prowadziło czynności. Pozyskiwanie informacji od prokuratury lub sądu o zakończeniu postępowania stanowi niezbędny element, umożliwiający rozpoczęcie procedury opisanej w przywołanym przepisie *ustawy o CBA*. Należy podkreślić, że wytyczne, stanowiące metodykę przeprowadzania poszczególnych etapów tej procedury, w obszarze wewnętrznych uregulowań prawnych wypełniają lukę, umożliwiając jednocześnie sprawną i kompleksową realizację usuwania danych wrażliwych.

Mając na uwadze, że proces zarządzania ryzykiem posiada kluczowe znaczenie w aspekcie bezpieczeństwa danych osobowych przetwarzanych przez CBA, Pełnomocnik przeprowadził analizę ryzyka wszystkich wyodrębnionych zbiorów danych osobowych. Miała ona na celu zidentyfikowanie ryzyk, na jakie narażone są dane przetwarzane w CBA, inaczej oszacować prawdopodobieństwo wystąpienia określonych zagrożeń wykorzystujących zidentyfikowane podatności, oraz określić prawdopodobieństwo wystąpienia oraz ich wpływ na bezpieczeństwo przetwarzania danych osobowych, a także opisać obszary wymagające zabezpieczenia i zastosowania środków ochrony. W konsekwencji analiza ryzyka ma pozwolić – za pomocą odpowiedniego doboru zabezpieczeń – na efektywną ochronę przed zidentyfikowanymi zagrożeniami poprzez kontrolowanie, unikanie lub minimalizowanie skutków zamierzonych lub przypadkowych zdarzeń mających wpływ na bezpieczeństwo przetwarzanych danych.

Analiza ryzyka, przeprowadzona metodą jakościową, wykazała, że zidentyfikowane ryzyka pozostają na poziomie akceptowalnym, dodatkowo stwierdzono istnienie ryzyk szczątkowych, które również zostały zaakceptowane. Zgodnie z obowiązującymi standardami w zakresie zarządzania bezpieczeństwem informacji przeprowadzona analiza ryzyka traktowana jest jako element całego systemu, który przewiduje okresowe jej przeprowadzanie, stałe monitorowanie ryzyk, wyznaczenie osób odpowiedzialnych za zarządzanie ryzykiem, szkolenia zarówno osób odpowiedzialnych za bezpieczeństwo przetwarzanych danych osobowych, jak i osób upoważnionych do dostępu do nich, oraz weryfikację wprowadzonych środków bezpieczeństwa, których utrzymanie na zakładanym poziomie gwarantuje ich skuteczność.

Pełnomocnik podejmuje również współpracę z innymi służbami mającą na celu podwyższanie świadomości istoty ochrony danych osobowych w ramach realizowanych zadań. Można do niej zaliczyć jego udział w VI Krajowym Forum Kierowników Jednostek Organizacyjnych oraz VIII Forum Pełnomocników ds. Ochrony Informacji Niejawnych, zorganizowanych przez Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego w dniach 20-22 listopada 2013 r. w Zakopanem. Honorowy patronat nad forami sprawowali: Biuro Bezpieczeństwa Narodowego, Służba Kontrwywiadu Wojskowego, Generalny Inspektor Ochrony Danych Osobowych oraz Krajowa Izba Gospodarcza.

Przedstawiciele Pełnomocnika odpowiedzialni za szkolenia oraz kontrole z zakresu ochrony danych osobowych wzięli też udział w konferencji naukowej „Publicznoprawne ograniczenia jawności. Zagadnienia wybrane", zorganizowanej w dniu 5 grudnia 2013 r. przez Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie w ramach projektu badawczo-rozwojowego pod nazwą „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym", współfinansowanego ze środków Narodowego Centrum Badań i Rozwoju. Celem konferencji była diagnoza aktualnych problemów stosowania prawa związanych z publicznoprawnymi ograniczeniami jawności oraz analiza instrumentów prawa publicznego zorientowanych na reglamentację dostępu do informacji i uruchomienie odpowiednich sankcji.

## III. PODSUMOWANIE

### 1. Ocena stanu ochrony danych osobowych

Systematyczny wzrost zapytań jednostek organizacyjnych Biura o interpretację obowiązujących w obszarze ochrony danych osobowych przepisów prawa, należy ocenić – w kontekście podwyższenia poziomu świadomości ochrony przetwarzanych danych w różnych aspektach aktywności CBA – pozytywnie. Można to uznać za rezultat aktywności i zaangażowania Pełnomocnika, polegających nie tylko na udzielaniu porad prawnych czy opracowywaniu wytycznych, ale także na organizacji szkoleń poświęconych tej tematyce. Nie można też zapomnieć o pozytywnym wymiarze przeprowadzonych kontroli, które – oprócz wykrywania nieprawidłowości czy uchybień w kontrolowanym zakresie – mają na celu popularyzację zasad ochrony danych osobowych i prawa do prywatności.

W wyniku dotychczas prowadzonych działań, przede wszystkim kontroli i sprawowaniu nadzoru nad weryfikacją niezbędności przetwarzania danych osobowych, należy uznać, że utworzony w CBA system przetwarzania danych osobowych gwarantuje kompleksową ich ochronę zgodną z obowiązującymi w tym zakresie przepisami, co stanowi podstawę pozytywnej oceny stanu ochrony danych osobowych w CBA.

W szczególności należy podkreślić, że:

- system ochrony danych osobowych w CBA jest spójny i obejmuje kompleksowo wszystkie obszary przetwarzania danych osobowych;
- od dnia powołania Pełnomocnika nie stwierdzono naruszeń ustawowych przepisów ochrony danych osobowych;
- funkcjonariusze i pracownicy CBA, upoważnieni do przetwarzania danych osobowych, mogą przetwarzać te dane wyłącznie w zakresie ustalonym indywidualnie w upoważnieniu i tylko w celu wykonywania nałożonych na nich obowiązków służbowych;
- dane osobowe (także sensytywne) są przetwarzane w CBA zgodnie z zasadą legalności;
- dane osobowe przetwarzane w CBA podlegają weryfikacji zgodnie z zasadą adekwatności, której celem jest wyodrębnienie i usunięcie tych danych osobowych, których przetwarzanie nie jest niezbędne do realizacji zadania;
- dane osobowe przetwarzane w CBA, w szczególności także w systemach teleinformatycznych, są odpowiednio zabezpieczone przed nieuprawnionym dostępem, a ich przetwarzanie odbywa się z wykorzystaniem środków i metod gwarantujących bezpieczną eksploatację.

Na koniec należy podkreślić, że – w związku z funkcjonowaniem Pełnomocnika jako gwaranta ochrony danych osobowych – od kilku lat w CBA nieustannie podwyższany jest poziom świadomości i pozytywnej aktywności w podejściu do zagadnień ochrony danych osobowych w służbie specjalnej. Zjawisko to stanowi podstawę „kultury przetwarzania danych osobowych", rozumianej nie tylko systemowo w zakresie rozwiązań organizacyjno-prawnych i technicznych, ale przede wszystkim odnoszącej się w mikroskali do codziennego przetwarzania danych osobowych poprzez właściwe nawyki funkcjonariuszy i pracowników, dotyczące m.in. potrzeby codziennej weryfikacji i usuwania danych zbędnych, utrzymywania porządku w środowisku pracy, a także przekonania, że realizacja zadania zgodnie z procedurą, wynikającą z przepisów resortowych, stanowi o prawidłowym przetwarzaniu danych zgodnie z zasadami, których źródło znajduje się w przepisach o ochronie danych osobowych.

## 2. Plany na rok 2014

W 2014 r. nadal priorytetowym zadaniem oprócz nadzoru nad dokonywaną weryfikacją i usuwaniem zbędnych danych osobowych będą kontrole prawidłowości przetwarzania danych osobowych w CBA. Na 2014 r. zaplanowano przeprowadzenie 5 kontroli kompleksowych z zakresu ochrony danych osobowych w wytypowanych jednostkach organizacyjnych CBA oraz jedną kontrolę problemową.

W połowie roku planuje się zorganizowanie konferencji dotyczącej ochrony danych osobowych dla funkcjonariuszy i pracowników CBA realizujących zadania związane z tym zakresem, jak również zaproszonych gości spoza Biura.

Ponadto – w ramach sprawowanego nadzoru nad funkcjonowaniem ochrony danych osobowych w CBA – Pełnomocnik nadal będzie podejmował działania w celu udoskonalania systemu ochrony. System ochrony danych osobowych w CBA wprowadzony regulacjami wewnętrznymi w 2011 r. pozwolił w roku sprawozdawczym na pełną realizację ustawowych obowiązków Pełnomocnika. Niemniej jednak zgromadzone w okresie trzech lat doświadczenia pozwalają poddać obecny system ocenie weryfikującej faktyczną jego funkcjonalność w stosunku do zakładanych oczekiwań oraz dostrzec elementy warte dopracowania. W związku z tym na rok 2014 zaplanowano przegląd dotychczas obowiązujących regulacji wewnętrznych dotyczących ochrony danych osobowych w CBA oraz przeprowadzenie procesu ich nowelizacji. Proces nowelizacyjny obejmie również decyzję w sprawie sposobu prowadzenia kontroli przetwarzania danych osobowych, który będzie miał na celu ujednolicenie sposobu postępowania z procedurą kontroli stanu ochrony informacji niejawnych.

Do zadań Pełnomocnika nadal będzie należało:

- wyjaśnianie potencjalnych incydentów dotyczących naruszeń przepisów o ochronie danych osobowych,
- dokonywanie okresowej analizy zagrożeń dla bezpieczeństwa danych osobowych, w wyniku której będą wdrażane zmiany w obowiązującej polityce bezpieczeństwa ochrony danych osobowych w CBA, w celu zapewnienia właściwego poziomu ochrony przetwarzanych danych osobowych,
- zarządzanie ryzykiem bezpieczeństwa danych osobowych (szacowania ryzyka dla poszczególnych zbiorów danych osobowych),
- podwyższanie poziomu kultury przetwarzania danych osobowych w CBA poprzez szkolenia i kampanie informacyjne,
- monitoring rozwiązań technologicznych wynikających z konieczności podwyższania poziomu zabezpieczeń fizycznych i teleinformatycznych w związku z nowymi rodzajami zagrożeń, a także pomoc w ich wdrażaniu,
- monitoring rozwiązań prawnych dotyczących ochrony danych osobowych, ze szczególnym uwzględnieniem przepisów kwestionowanych ze względu na niedostateczne zapewnienie ochrony danych osobowych, przetwarzanych w celu realizacji ustawowych zadań służby.

Pełnomocnik
do spraw kontroli przetwarzania
przez CBA danych osobowych
*Maciej Malerka*

Wykonano w 4 egzemplarzach:
Egz. nr 1 – Prezes Rady Ministrów Pan Donald Tusk
Egz. nr 2 – Przewodnicząca Sejmowej Komisji do Spraw Służb Specjalnych Pani Elżbieta Radziszewska
Egz. nr 3 – Generalny Inspektor Ochrony Danych Osobowych Pan Wojciech Rafał Wiewiórowski
Egz. nr 4 – ad acta