



Komendant  
Centrum Szkolenia Straży Granicznej  
im. Żołnierzy Korpusu Ochrony Pogranicza

Kętrzyn, dnia 14 lipca 2017 r.

CS-NK.0910.2.2017

Egz. Nr 2...

kpt. SG Tomasz BIENIEK

**KIEROWNIK SAMODZIELNEJ SEKCJI  
PEŁNOMOCNIK KOMENDANTA  
CENTRUM SZKOLENIA STRAŻY GRANICZNEJ  
Ds. Ochrony Informacji Niejawnych**

### WYSTĄPIENIE POKONTROLNE

z kontroli zgodnej z rocznym planem kontroli, zrealizowanej w trybie zwykłym.

Kontrola została przeprowadzona na podstawie *Wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub w jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych* stanowiących załącznik do Decyzji nr 65 Ministra Spraw Wewnętrznych z dnia 31 maja 2012 r. w sprawie wprowadzenia do stosowania wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub w jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych<sup>1</sup> w związku z § 1 Decyzji nr 139 Komendanta Głównego Straży Granicznej z dnia 30 sierpnia 2012 w sprawie wprowadzenia do stosowania w Straży Granicznej wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub w jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych<sup>2</sup>.

#### I. Temat kontroli:

Sprawowanie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, przetwarzanych w Centrum Szkolenia Straży Granicznej.

#### II. Podmiot kontrolowany:

1. Oznaczenie podmiotu kontrolowanego: Samodzielna Sekcja Ochrony Informacji<sup>3</sup> Centrum Szkolenia Straży Granicznej, 11-400 Kętrzyn, ul. Gen. Władysława Sikorskiego 78<sup>4</sup>;
2. Kierownik podmiotu kontrolowanego: kpt. SG Tomasz Bieniek – Kierownik Samodzielnej Sekcji Pełnomocnik Komendanta CSSG ds. Ochrony Informacji Niejawnych CSSG<sup>5</sup>.

<sup>1</sup> Dz. Urz. MSW z 2012 r. poz. 43 z późn. zm. – zwane dalej wytycznymi.

<sup>2</sup> Dz. Urz. KGSG z 2012 r. poz. 47 z późn. zm.

<sup>3</sup> Zwana dalej SSOI.

<sup>4</sup> Zwane dalej CSSG.

Funkcję kierownika podmiotu kontrolowanego w okresie objętym kontrolą pełnił kpt. SG Tomasz Bieniek.

**III. Imię i nazwisko, stanowisko służbowe kontrolerów, nazwa komórki kontroli oraz numer i data upoważnienia do kontroli z uwzględnieniem zmian w okresie prowadzenia kontroli:**

1. kierownik zespołu kontrolnego:
  - a) kpt. SG Katarzyna Pejda – starszy specjalista - koordynator Referatu Kontroli w Kierownictwie CSSG, upoważnienie nr 3/2017 z dnia 14.04.2017 r.;
2. członek zespołu kontrolnego:
  - a) Sebastian Dunaj – starszy specjalista Referatu Kontroli w Kierownictwie CSSG, upoważnienie nr 4/2017 z dnia 14.04.2017 r.

**IV. Data rozpoczęcia i zakończenia czynności kontrolnych w podmiocie kontrolowanym, z wymienieniem dni przerw w kontroli:**

1. Data rozpoczęcia czynności kontrolnych: 18.04.2017 r.;
2. Data zakończenia czynności kontrolnych: 26.05.2017 r.;

**V. Zakres kontroli:**

1. Przedmiot kontroli:

- 1) prawidłowość prowadzenia wykazu zbiorów danych osobowych przetwarzanych w CSSG,
- 2) prawidłowość realizacji przez ABI/ZABI zadań określonych w Decyzji Nr 18 Komendanta CSSG,
- 3) prawidłowość realizacji przez ABZ zadań określonych w Decyzji Nr 18 Komendanta CSSG,
- 4) prawidłowość realizacji przez ATI zadań określonych w Decyzji Nr 18 Komendanta CSSG,
- 5) realizacja obowiązku przeprowadzania szkoleń funkcjonariuszy i pracowników CSSG z zakresu ochrony danych osobowych w CSSG,
- 6) realizacja wymagań w zakresie przetwarzania danych osobowych, określonych w obowiązujących przepisach, dotyczących ochrony danych osobowych,
- 7) stosowanie środków technicznych i organizacyjnych, niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych,
- 8) stosowanie „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w CSSG”.

2. Okres objęty kontrolą:

Kontrolą objęto okres od 01.01.2016 r. do 17.04.2017 r.

**VI. Cel kontroli:**

Celem kontroli była ocena na podstawie ustalonego stanu faktycznego, przy zastosowaniu przyjętych kryteriów kontroli:

---

<sup>5</sup> Zwany dalej Kierownikiem SSOI.

- prawidłowości prowadzenia wykazu zbiorów danych osobowych przetwarzanych w CSSG;
- prawidłowości realizacji przez Administratora Bezpieczeństwa Informacji Komendanta CSSG<sup>6</sup>/Zastępcę Administratora Bezpieczeństwa Informacji Komendanta CSSG<sup>7</sup> zadań określonych w Decyzji Nr 18 Komendanta CSSG z dnia 14 marca 2016 r. w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w CSSG<sup>8</sup>;
- prawidłowości realizacji przez Administratora Bezpieczeństwa Zbioru CSSG<sup>9</sup> zadań określonych w Decyzji Nr 18 Komendanta CSSG;
- prawidłowości realizacji przez Administratora Systemu Teleinformatycznego<sup>10</sup> zadań określonych w Decyzji Nr 18 Komendanta CSSG;
- realizacji obowiązku przeprowadzania szkoleń funkcjonariuszy i pracowników CSSG z zakresu ochrony danych osobowych w CSSG;
- realizacji wymagań w zakresie przetwarzania danych osobowych, określonych w obowiązujących przepisach, dotyczących ochrony danych osobowych;
- stosowania środków technicznych i organizacyjnych, niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
- stosowania „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w CSSG”.

Celem kontroli było również ustalenie zakresu, przyczyn i skutków oraz osób odpowiedzialnych za ewentualnie stwierdzone nieprawidłowości, a także sformułowanie zaleceń zmierzających do ich usunięcia.

Sformułowanie oceny realizacji zadań przez podmiot kontrolowany, objętych zakresem kontroli nie było oparte na próbie, gdyż czynnościom kontrolnym zostało poddane 100% dokumentacji związanej z przedmiotem kontroli.

Czynności kontrolne zrealizowano w zakresie kontroli prawidłowości przy zastosowaniu kryteriów kontroli: legalność, celowość i rzetelność.

## **VII. Ocena skontrolowanej działalności ze wskazaniem ustaleń na których została oparta. Zakres, przyczyny i skutki stwierdzonych nieprawidłowości oraz wskazanie osób za nie odpowiedzialnych:**

Oceny realizacji zadań objętych zakresem kontroli dokonano na podstawie przepisów prawa oraz faktycznych ustaleń kontroli poczynionych w oparciu o dokumenty zgromadzone przez kontrolerów, udostępnione kontrolerom oraz wyjaśnienia i informacje uzyskane od kierownika i pracowników podmiotu kontrolowanego oraz pozyskane od pracowników z innych podmiotów niż kontrolowany w zakresie objętym kontrolą (udokumentowanych w aktach kontroli).

<sup>6</sup> Zwany dalej ABI.

<sup>7</sup> Zwany dalej ZABI.

<sup>8</sup> Zwana dalej Decyzją Nr 18 Komendanta CSSG.

<sup>9</sup> Zwany dalej ABZ.

<sup>10</sup> Zwany dalej ATI.

Uwzględniając czynniki takie jak: zakres kontroli i okres objęty kontrolą, na podstawie czterostopniowej skali, obejmującej ocenę: pozytywną, pozytywną z uchybieniami, pozytywną z nieprawidłowościami oraz negatywną, realizację zadań przez podmiot kontrolowany oceniono pozytywnie z nieprawidłowościami.

Na powyższą ocenę końcową złożyły się oceny cząstkowe poszczególnych obszarów poddanych kontroli, sformułowane na podstawie ustalonego w trakcie kontroli stanu faktycznego, opisanego poniżej:

1. Prawidłowość prowadzenia wykazu zbiorów danych osobowych przetwarzanych w CSSG.

Zgodnie z treścią art. 6 ust. 1 Ustawy z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych*<sup>11</sup> za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (art. 6 ust. 2 uodo). Natomiast w myśl art. 6 ust. 3 uodo informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Pod pojęciem zbioru danych w/w ustawa rozumie każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie (art. 7 pkt 1 uodo). W treści art. 7 pkt 2 uodo zawarto definicję ustawową pojęcia przetwarzanie danych, przez co rozumie się jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Tematyka wykazów zbiorów danych osobowych przetwarzanych w jednostkach organizacyjnych Straży Granicznej została uregulowana w n/w aktach prawnych:

- a) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. *w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych*<sup>12</sup>;
- b) Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. *w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji*<sup>13</sup>;
- c) Decyzja Nr 129 Komendanta Głównego Straży Granicznej<sup>14</sup> z dnia 11 czerwca 2014 r. *w sprawie ochrony danych osobowych przetwarzanych w Straży Granicznej*<sup>15</sup> zmieniona Decyzją Nr 271 Komendanta Głównego Straży Granicznej z dnia 09 grudnia 2015 r.

<sup>11</sup> t.j. Dz. U. z 2016 r. poz. 922, zwana dalej uodo

<sup>12</sup> Dz. U. z 2015 r. poz. 719, zwane dalej rozporządzeniem w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych.

<sup>13</sup> Dz. U. z 2015 r. poz. 745, zwane dalej rozporządzeniem w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

<sup>14</sup> Zwany dalej Komendantem Głównym SG.

<sup>15</sup> Dz. Urz. KGSG z 2014 r. poz. 90, zwana dalej decyzją Nr 129 Komendanta Głównego SG.

zmieniającą decyzję w sprawie ochrony danych osobowych przetwarzanych w Straży Granicznej<sup>16</sup>;

- d) Decyzja Nr 11 Komendanta Centrum Szkolenia Straży Granicznej<sup>17</sup> z dnia 04 maja 2011 r. w sprawie zabezpieczenia danych osobowych, których administratorem jest Komendant Centrum Szkolenia Straży Granicznej<sup>18</sup> oraz wskazane w w/w decyzji „Polityka bezpieczeństwa przetwarzania danych osobowych w Centrum Szkolenia Straży Granicznej” i „Regulamin przetwarzania danych osobowych w zbiorach tradycyjnych Centrum Szkolenia Straży Granicznej” (obowiązujące do dnia 13 marca 2016 r.);
- e) Decyzja Nr 18 Komendanta CSSG z dnia 14 marca 2016 r. w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Centrum Szkolenia Straży Granicznej<sup>19</sup> oraz wprowadzona w/w decyzją „Polityka bezpieczeństwa danych osobowych w Centrum Szkolenia Straży Granicznej” (od dnia 14 marca 2016 r.);

Przed wejściem w życie Decyzji Nr 271 Komendanta Głównego SG opis struktury wykazu zbiorów danych wskazany był w § 4 ust. 1 i 2 decyzji Nr 129 Komendanta Głównego SG.

Zauważyć należy, że rozporządzenie w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych weszło w życie w dniu 26 maja 2015 r., natomiast do wewnętrznych przepisów dotyczących ochrony danych osobowych w Straży Granicznej<sup>20</sup> zaimplementowane zostało dopiero decyzją Nr 271 Komendanta Głównego SG, która weszła w życie w dniu 17 grudnia 2015 r. Uregulowania w zakresie ochrony danych osobowych wynikające z w/w aktów prawnych w CSSG zostały wprowadzone decyzją Nr 18 Komendanta CSSG z dnia 14 marca 2016 r. Powyższe prowadzi do wniosku, że przepisy rozporządzenia w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych nie były realizowane w CSSG przez okres niemal roku od ich wydania. Wskazać warto, że w decyzji Nr 271 Komendanta Głównego SG przewidziano 7 dniowy okres *vacatio legis* umożliwiający wprowadzenie jej zapisów w poszczególnych jednostkach organizacyjnych SG, w którym to okresie winny być wydane przepisy ujednolicające przepisy dotyczące ochrony danych osobowych w poszczególnych jednostkach organizacyjnych SG z przepisami wydanymi przez Komendanta Głównego SG. Ostatecznie „Wykaz zbiorów danych osobowych przetwarzanych w CSSG” został zatwierdzony przez Komendanta CSSG w dniu 12 maja 2016 r.<sup>21</sup>

W wyjaśnieniach z dnia 27 kwietnia 2017 r. ██████████<sup>22</sup> wskazał, że prace nad nowym wykazem zbioru danych osobowych przetwarzanych w CSSG zostały rozpoczęte w sierpniu, po powrocie ██████████ w czerwcu ze zwolnienia lekarskiego i po wykorzystaniu urlopu wypoczynkowego. Równoległe do prac nad nowym zbiorem danych osobowych ██████████ rozpoczęła prace nad nową decyzją w sprawie przetwarzania danych osobowych oraz Polityką bezpieczeństwa w CSSG. Kierownik SSOI wskazał, że po wejściu w życie noweli decyzji Nr 129 Komendanta Głównego SG

<sup>16</sup> Dz. Urz. KGSG z 2015 r. poz. 92, zwana dalej decyzją Nr 271 Komendanta Głównego SG.

<sup>17</sup> Zwanego dalej Komendantem CSSG.

<sup>18</sup> Zwana dalej decyzją Nr 11 Komendanta CSSG.

<sup>19</sup> Zwana dalej decyzją Nr 18 Komendanta CSSG.

<sup>20</sup> Zwanej dalej SG.

<sup>21</sup> dowód, akta kontroli – karty nr 20-57.

<sup>22</sup> dowód, akta kontroli – karty nr 17-18.

dopracowane zostały projekty aktów prawnych i 14 marca 2016 r. weszła w życie decyzja Nr 18 Komendanta CSSG, a 12 maja zatwierdzony został przez Komendanta CSSG „Wykaz zbiorów danych osobowych przetwarzanych w CSSG”.

W ocenie zespołu kontrolnego nie zachodziły żadne okoliczności uzasadniające zwłokę w opracowaniu dokumentów dotyczących ochrony danych osobowych w CSSG w sposób zgodny ze znowelizowanymi przepisami. Zaniechanie opracowania nowych dokumentów w okresie od wejścia w życie decyzji Nr 271 Komendanta Głównego SG, tj. od dnia 17 grudnia 2015 r. do dnia 12 maja 2016 r., nawet pomimo wydania Decyzji Nr 18 Komendanta CSSG stanowi uchybienie, za które odpowiedzialność ponosi Kierownik SSOI – ██████████, który zgodnie z pkt II.31 Szczegółowego zakresu obowiązków i uprawnień Kierownika SSOI opiniuje oraz przedstawia propozycje projektów aktów normatywnych w zakresie właściwości sekcji. Ponadto, zgodnie z treścią § 16 ust 2 pkt 9 Załącznika Nr 1 do Decyzji Nr 18 Komendanta CSSG „Polityka bezpieczeństwa przetwarzania danych osobowych w CSSG”<sup>23</sup>, Administrator bezpieczeństwa informacji którym jest Kierownik SSOI ██████████ prowadzi „Rejestr zbiorów danych osobowych przetwarzanych w CSSG” oraz „Wykaz zbiorów danych osobowych przetwarzanych w CSSG”. Stosowanie do zapisu zawartego w § 16 ust 3 Polityki bezpieczeństwa ABI realizuje zadania przy pomocy zastępcy ABI oraz innych funkcjonariuszy i pracowników mu podległych. Zgodnie z pkt 5 i 9 Szczegółowego zakresu obowiązków i uprawnień ██████████ do zadań jej powierzonych do realizacji należy opracowywanie, wdrażanie i aktualizowanie Polityki bezpieczeństwa przetwarzania danych osobowych CSSG oraz prowadzenie „Wykazu zbiorów danych osobowych przetwarzanych w CSSG”<sup>24</sup>. Zaniechanie opracowania „Wykazu zbiorów danych osobowych przetwarzanych w CSSG” niezwłocznie po wydaniu Polityki bezpieczeństwa stanowi zatem uchybienie, za które odpowiedzialna jest ██████████ - ██████████.

Na marginesie zespół kontrolny zauważa błędne odesłanie zawarte w § 15 ust. 4 decyzji nr 18 Komendanta CSSG do osób funkcyjnych, o których mowa w § 13 pkt 2-7, które *de facto* wymienione są w § 14 pkt 2-7. Ponadto zespół kontrolny stoi na stanowisku, że przedmiotowa decyzja w § 20 ust. 1 niezasadnie zawęża przetwarzanie danych osobowych w CSSG w zbiorach danych zawartych w wykazie zbiorów i utworzonych przez Komendanta CSSG – w celu i zakresie, w jakim zbiory danych zostały utworzone, nie odnosząc się do zbiorów danych osobowych udostępnionych przez Komendanta Głównego SG. Na dzień dzisiejszy w CSSG istnieje 5 zbiorów danych osobowych, których administratorem danych jest Komendant Główny SG.

W toku czynności kontrolnych kontroli poddano opracowany przez ██████████ „Rejestr zbiorów danych osobowych przetwarzanych w CSSG” zatwierdzony przez Komendanta CSSG w dniu 01 grudnia 2015 r. (Nr 2117/15), obowiązujący w okresie objętym kontrolą do czasu zatwierdzenia nowego wykazu zbiorów danych osobowych, tj. do dnia 11 maja 2016 r.

Wzór „Wykazu zbiorów danych osobowych przetwarzanych w CSSG” został określony w załączniku nr 1 do „Polityki Bezpieczeństwa przetwarzania danych osobowych w CSSG” wprowadzonej decyzją Nr 11 Komendanta CSSG.

<sup>23</sup> Zwany dalej „Polityką bezpieczeństwa”.

<sup>24</sup> dowód, akta kontroli – karta nr 82.

W wyniku porównania „Rejestru zbiorów danych osobowych przetwarzanych w CSSG” z wzorem określonym w załączniku do Polityki bezpieczeństwa zespół kontrolny ujawnił n/w rozbieżności w zakresie:

- nazwy dokumentu, gdyż zamiast wskazanego w Polityce bezpieczeństwa „Wykazu zbiorów danych osobowych przetwarzanych w CSSG” (zob. I. pkt 4 ppkt 17 Polityki bezpieczeństwa wprowadzonej decyzją Nr 11 Komendanta CSSG) do kontroli przedłożono „Rejestr zbiorów danych osobowych przetwarzanych w CSSG”;
- rubryk wskazanych w „Wykazie zbiorów danych osobowych przetwarzanych w CSSG” i w przedłożonym do kontroli dokumencie „Rejestr zbiorów danych osobowych przetwarzanych w CSSG” (ilość i nazwy poszczególnych rubryk).

Powyższe prowadzi do wniosku, że „Wykaz zbiorów danych osobowych przetwarzanych w CSSG” prowadzony był w sposób niezgodny z załącznikiem nr 1 Polityki bezpieczeństwa wprowadzonej decyzją Nr 11 Komendanta CSSG. Stanowi to uchybienie, za które odpowiedzialność ponosi Kierownik SSOI [REDAKTOWANE], przy czym, w ocenie zespołu kontrolnego, uchybienie to nie wywołało negatywnych skutków.

Z uwagi na to, że w/w Decyzja obowiązywała w okresie objętym kontrolą, ale tylko do dnia 13 marca 2016 r. a w chwili obecnej całość dokumentacji dotyczącej ochrony danych osobowych w CSSG jest nieaktualna ze względu na nowe uregulowania prawne, zespół kontrolny dokonał kontroli tylko w zakresie nowych uregulowań prawnych, z pominięciem przepisów już nieobowiązujących.

W dalszej kolejności zespół kontrolny poddał kontroli „Wykaz zbiorów danych osobowych przetwarzanych w CSSG” zatwierdzony przez Komendanta CSSG w dniu 12 maja 2016 r. (Rtd nr 11/17). Czynności kontrolne ujawniły, że w „Historii zmian dokonanych w wykazie” nie zawarto adnotacji dotyczących usunięcia zbioru nr 4/WZSDCSSG o nazwie „Ewidencja osób przeszkolonych w zakresie ochrony danych osobowych/Rejestr wydanych zaświadczeń”, który został włączony jako podzbiór do zbioru „Szkolenia SSOI CSSG” oraz zbioru Nr 16/WZDCSSG o nazwie „Wykaz pracowników i funkcjonariuszy w zakresie okresowych wstępnych badań lekarskich i w zakresie okresowych szkoleń BHP” który został włączony jako podzbiór do zbioru „Bezpieczeństwo i higiena pracy”. Sposób dokonania w/w zmian uniemożliwia jednoznaczne stwierdzenie, czy w „Wykazie zbiorów danych osobowych przetwarzanych w CSSG” znajdują się aktualne arkusze wykazu zbiorów danych osobowych. W momencie tworzenia „Wykazu zbiorów danych osobowych przetwarzanych w CSSG” nie została zachowana ciągłość numeracji zbiorów danych osobowych. W ocenie zespołu kontrolnego tworząc nowy dokument „Wykaz zbiorów danych osobowych przetwarzanych w CSSG” należało zachować kolejność numeracji poszczególnych zbiorów, co pozwoliłoby na uniknięcie wątpliwości dotyczących jednolitości analizowanego dokumentu. Jeżeli natomiast, jak miało to miejsce w przypadku usunięcia zbioru Nr 16/WZDCSSG o nazwie „Wykaz pracowników i funkcjonariuszy w zakresie okresowych wstępnych badań lekarskich i w zakresie okresowych szkoleń BHP”, który został włączony jako podzbiór do zbioru „Bezpieczeństwo i higiena pracy”, do usunięcia zbioru doszło już po zatwierdzeniu „Wykazu zbiorów danych osobowych przetwarzanych w CSSG” przez Komendanta CSSG, powinno to zostać odnotowane w „Historii zmian dokonanych w wykazie”, gdzie winien być szczegółowo opisany zakres dokonanych zmian dokumentu. Powyższe jest niezgodne ze sposobem postępowania związanym z odnotowywaniem zmian w rejestrze, określonym w § 6 rozporządzenia

w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych.

Ponadto analiza „Wykazu zbiorów danych osobowych przetwarzanych w CSSG” oraz „Rejestru zbiorów danych osobowych przetwarzanych w CSSG” (zatwierdzony przez Komendanta CSSG w dniu 12.05.2016 r. Rtd nr 11/17) prowadzi do wniosku, że w/w dokumenty zastały skopiowane z odpowiednich dokumentów opracowanych przez Komendę Główną SG. Na powyższe wskazuje treść nagłówka w tabeli wskazanej w pkt 8 „Wykaz zbiorów danych osobowych” oraz pkt 5 „Rejestr zbiorów danych osobowych” i „Rejestr zbiorów danych osobowych przetwarzanych w CSSG” (str. 3 Rejestru). W w/w przypadkach, we wszystkich nagłówkach tabel widnieje ta sama nazwa, tj. „Rejestr zbiorów danych osobowych których administratorem jest Komendant CSSG lub kierownicy jednostek organizacyjnych SG z wyłączeniem zbiorów, których prowadzenie zakończono i zarchiwizowano bądź zostały włączone do centralnych baz danych”. W wyjaśnieniach z dnia 22 maja 2017 r. [REDAKTOWANE]<sup>25</sup> nazwę nagłówków tabel tłumaczy tym, że w rejestrze mogą znajdować się (w przyszłości) lub znajdują się zbiory, których administratorem jest Komendant CSSG, jak również zbiory udostępnione CSSG przez innych administratorów danych osobowych jednostek organizacyjnych SG. W pierwszej kolejności należy wskazać, że w przedmiotowym wykazie wymienione są także zbiory, gdzie z „Arkusza wykazu zbiorów danych przetwarzanych w CSSG” wynika że administratorem zawartych w nich danych jest Komendant Główny SG. Dotyczy to zbiorów danych: „CBD SG Kadry”, „Rejestr skarg i wniosków”, „Wykaz przedmiotów przekazanych komendzie Głównej Straży Granicznej na mocy prawomocnych orzeczeń o ich przepadku”, „Centralna Baza danych Straży Granicznej System Wspomagania Kierowania (CBD SG SWK)”, „Archiwum Straży Granicznej” oraz „Rejestr przyjęć interesantów w sprawach skarg i wniosków”. W ocenie zespołu kontrolnego ABZ winna była, w ramach „Wykazu zbiorów danych osobowych ...”, wyodrębnić zbiory danych osobowych, których administratorem jest Komendant CSSG od zbiorów danych powierzonych do przetwarzania Komendantowi CSSG przez Komendanta Głównego SG, co wynika z § 13 ust. 3 Polityki bezpieczeństwa nakazującego wyodrębnienie zbiorów danych, których administratorem jest Komendant CSSG od zbiorów danych udostępnionych przez inne podmioty Komendantowi CSSG. Powyżej wskazany sposób wyodrębnienia zbiorów ułatwił ABI prawidłowe nadawanie upoważnień do przetwarzania danych zgromadzonych w poszczególnych zbiorach i poprawił przejrzystość dokumentu.

Warto także wskazać, że omawiane nagłówki tabel zawierają błędne określenie administratora danych osobowych w sytuacji, gdy obok Komendanta CSSG (prawidłowe) wskazani są kierownicy jednostek organizacyjnych SG (niezrozumiałe). Ponadto błędne jest nazywanie nagłówka tabeli „Rejestr zbiorów danych osobowych ...” w sytuacji, gdy jest to „Wykaz zbiorów danych osobowych ...” (str. 3), mając na względzie, że są to dwa odrębne dokumenty.

Powyższe stanowi uchybienie, za które odpowiedzialność ponosi [REDAKTOWANE], która zgodnie z pkt II.5 i II.9 Szczegółowego zakresu obowiązków i uprawnień [REDAKTOWANE] [REDAKTOWANE] odpowiedzialna jest za opracowywanie, wdrażanie i aktualizowanie

<sup>25</sup> dowód, akta kontroli – karty nr 74-81.



Polityki bezpieczeństwa przetwarzania danych osobowych CSSG oraz prowadzenie „Wykazu zbiorów danych osobowych przetwarzanych w CSSG”<sup>26</sup>.

W myśl § 2 ust. 1 rozporządzenia w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych rejestr zbiorów danych składa się z wykazu zbiorów danych zawierającego informacje określone w § 3 odrębnie dla każdego zbioru danych. Ponadto, zgodnie z treścią § 4 ust. 1 decyzji Nr 271 Komendanta Głównego SG wykaz zbiorów danych stanowi odrębny dokument i zawiera w szczególności informacje, o których mowa w § 3 powyższego rozporządzenia. Dokonana przez zespół kontrolny analiza zapisów „Wykazu zbiorów danych osobowych przetwarzanych w CSSG” wykazała, że dokument zawiera wymagane w/w przepisami prawa informacje. Uwagę zespołu kontrolnego zwróciła używana zamiennie nazwa zbioru „Ewidencja kandydatów do służby i pracy” (nazwa wskazana w „Wykazie zbiorów danych osobowych przetwarzanych w CSSG”) i „Ewidencja kandydatów do służby przygotowawczej i pracy” (nazwa wskazana w „Arkuszu wykazu zbiorów danych osobowych przetwarzanych w CSSG”). W wyjaśnieniach z dnia 18 maja 2017 r. ██████████<sup>27</sup> wyjaśnił, iż właściwą nazwą jest „Ewidencja kandydatów do służby przygotowawczej i pracy” a nazwa podana w „Arkuszu wykazu zbiorów danych osobowych przetwarzanych w CSSG” jest omyłkowa.

W dalszej części kontroli zespół kontrolny dokonał analizy zapisów opracowanego przez ██████████ dokumentu „Wykaz budynków i pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w CSSG” (Nr 1202/16 z dnia 05.07.2017 r.), który jest powiązany z dokumentem „Wykaz zbiorów danych osobowych przetwarzanych w CSSG”, stanowiąc w myśl § 8 Polityki bezpieczeństwa integralną część „Polityki Bezpieczeństwa przetwarzania danych osobowych w CSSG”. W wyniku powyższego ustalono, iż w dokumencie „Wykaz budynków i pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w CSSG” wskazane są dwie błędne nazwy zbioru danych osobowych. Dotyczy to:

- lp. 11, gdzie widnieje nazwa zbioru „ Ewidencja kandydatów do służby i pracy” w sytuacji, gdy poprawną nazwą jest „Ewidencja kandydatów do służby przygotowawczej i pracy”,
- lp. 16, gdzie widnieje nazwa zbioru „Wykaz przedmiotów przekazanych KGSG na mocy prawomocnych orzeczeń o ukaraniu” w sytuacji, gdy poprawną nazwą jest „Wykaz przedmiotów przekazanych KGSG na mocy prawomocnych orzeczeń o ich przypadku”.

Zespół kontrolny porównując zapisy dokumentu „Wykaz budynków i pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w CSSG” z nadanymi funkcjonariuszom i pracownikom CSSG upoważnieniami do przetwarzania danych osobowych, ustalił, że w przedmiotowym dokumencie nie są ujęte wszystkie pomieszczenia, zajmowane przez osoby posiadające upoważnienia do przetwarzania danych osobowych, tj.: zawartych w zbiorze „Ewidencja kandydatów do służby i pracy” - pomieszczenia nr 320, zawartych w zbiorze „Książka obsady etatowej” - pomieszczenia nr 319. Na okoliczność powyższego ██████████ w dniu 25 maja 2017 r. złożył wyjaśnienia<sup>28</sup>, w których stwierdził, że w „Wykazie budynków i pomieszczeń ...” wskazane są wyłącznie pomieszczenia, w których przechowywane są zbiory danych osobowych, gdyż gdyby w wykazie były wymieniane wszystkie pomieszczenia, w których mogą być

<sup>26</sup> dowód, akta kontroli – karta nr 82.

<sup>27</sup> dowód, akta kontroli – karty nr 86-88 .

<sup>28</sup> dowód, akta kontroli – karty nr 90-93.

przetwarzane dane osobowe, to nikt nie byłby w stanie określić, gdzie faktycznie znajdują się zbiory danych, a taki jest cel prowadzenia w/w wykazu.

Ponadto zespół kontrolny ustalił, że w „Wykazie budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są zbiory danych osobowych” w zakresie przetwarzania danych osobowych w zbiorze „Rejestr słuchaczy” podzbiór „Lista uczestników kursu/szkolenia” ujęto sale wykładowe zajmowane przez Zakład Prawa i Kryminalistyki (sala 8 i 114 blok 27), natomiast pominięto inne sale usytuowane w pozostałych budynkach zajmowanych przez CSSG, w których prowadzone są zajęcia dydaktyczne z udziałem słuchaczy. Z wyjaśnień złożonych w dniu 25 maja 2017 r. przez [REDAKTOWANE] wynika, że przedmiotowy wpis został popełniony omyłkowo przez osobę prowadzącą „Wykaz pomieszczeń ...”. W trakcie kontroli, tj. w dniu 25 maja 2017 r., [REDAKTOWANE] dokonała wykreślenia z przedmiotowego dokumentu pomieszczeń nr 8 i 114 oraz budynku 27, wskazując, że powyższe wpisy były dokonane omyłkowo<sup>29</sup>. Dokonanie w/w zmiany prowadzi do wniosku, że w budynku 27 nie są obecnie przetwarzane w ogóle dane osobowe w zbiorze „Rejestr słuchaczy” podzbiór „Lista uczestników kursu/szkolenia”, co w ocenie zespołu kontrolnego, nie odpowiada rzeczywistości i pozostaje w sprzeczności z upoważnieniami nadanymi osobom pełniącym służbę w w/w budynku. Powyższe zmiany, z przyczyn nieznanych zespołowi kontrolnemu, zostały uwidocznione zarówno w „Wykazie pomieszczeń ...”, jak też w Aneksie Nr 1 i w Aneksie nr 2 do w/w dokumentu.

Powyższe stanowi uchybienie, za które odpowiedzialność ponosi [REDAKTOWANE], która zgodnie z § 17 ust 1 pkt 5 Polityki bezpieczeństwa oraz pkt II.8 Szczegółowego zakresu obowiązków i uprawnień Specjalisty ds. danych osobowych SSOI odpowiedzialna jest za prowadzenie „Wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w których są przetwarzane i przechowywane zbiory danych osobowych”<sup>30</sup>.

Zgodnie z treścią pkt 2 „Rejestru zbiorów danych osobowych przetwarzanych w CSSG” integralną częścią Rejestru są kopie arkuszy z „Wykazu zbiorów danych osobowych przetwarzanych w CSSG”. Tymczasem w toku czynności kontrolnych ujawniono, że w „Rejestrze zbiorów danych osobowych przetwarzanych w CSSG” znajdują się oryginały arkuszy z „Wykazu zbiorów danych osobowych przetwarzanych w CSSG”. Stanowi to uchybienie, za które odpowiedzialność ponosi Kierownik SSOI [REDAKTOWANE] oraz [REDAKTOWANE], przy czym, w ocenie zespołu kontrolnego, uchybienie te nie wywołało negatywnych skutków.

Powyższy obszar kontroli zespół kontrolny ocenił pozytywnie z uchybieniami.

## 2. Prawidłowość realizacji przez ABI/ZABI zadań określonych w Decyzji Nr 18 Komendanta CSSG.

Zgodnie z § 15 ust 1 Polityki bezpieczeństwa zadania ABI w CSSG wykonuje Kierownik SSOI. Natomiast, zgodnie z § 15 ust 2 Polityki bezpieczeństwa, zadania ZABI wykonuje wyznaczony funkcjonariusz lub pracownik SSOI. Decyzją Nr 1 Komendanta CSSG z dnia 20 stycznia 2015 r. do pełnienia funkcji Administratora Bezpieczeństwa Informacji Komendanta CSSG powołano [REDAKTOWANE] – Kierownika SSOI CSSG. Tą samą

<sup>29</sup> dowód, akta kontroli – karty nr 131-134 .

<sup>30</sup> dowód, akta kontroli – karta nr 82.

decyzją do pełnienia funkcji Zastępcy Administratora Bezpieczeństwa Informacji Komendanta CSSG powołano [REDAKTOWANE] – specjalistę SSOI CSSG<sup>31</sup>.

Zadania ABI/ZABI zostały szczegółowo określone w § 16 ust 1 pkt 5 Polityki bezpieczeństwa. Zespół kontrolny dokonał kontroli prawidłowości realizacji zadań określonych w Polityce bezpieczeństwa przez ABI. W wyjaśnieniach złożonych w dniu 16 maja 2017 r. [REDAKTOWANE]<sup>32</sup> wskazał, że zadanie polegające na zapewnieniu przestrzegania przepisów dotyczących przetwarzania danych osobowych jest realizowane poprzez dokonywanie sprawdzeń, zarówno planowanych jak i doraźnych, z których są sporządzane sprawozdania. Ponadto, poprzez przeprowadzanie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych, realizowany jest wymóg dotyczący zapoznania osób upoważnionych do przetwarzania danych osobowych z odpowiednimi przepisami. Dodatkowo, jak wynika ze złożonych wyjaśnień, na bieżąco prowadzona jest analiza zagrożeń dla bezpieczeństwa danych osobowych, której dokonuje zarówno ABI oraz ABZ w poszczególnych komórkach organizacyjnych.

Odnosnie obowiązku dotyczącego wydawania zaleceń w zakresie ochrony danych osobowych [REDAKTOWANE] w wyjaśnieniach z dnia 16 maja 2017 r.<sup>33</sup> wskazał, że zalecenia oraz pouczenia wydawane przez niego są zawarte w sprawozdaniach z przeprowadzonych sprawdzeń.

W ramach przeprowadzonej kontroli zespół kontrolny poddał analizie sprawdzenia przeprowadzone w okresie objętym kontrolą. Sprawdzenia, które udokumentowane zostały sprawozdaniami, realizowane były w Wydziale Zabezpieczenia Szkolenia (pismo nr 1004/16 z 07.06.2016 r.)<sup>34</sup>, Wydziale Kadr (pismo nr 1326/16 z dnia 22.07.2016 r.)<sup>35</sup> oraz w Pododdziałach Szkolnych CSSG (pismo nr 2171/16 z dnia 13.12.2016 r.)<sup>36</sup>. Uwagę zespołu kontrolnego wzbudziło sprawozdanie ze sprawdzenia przeprowadzonego w Wydziale Kadr z dnia 22 lipca 2016 r., w którym nie stwierdzono nieprawidłowości, natomiast w wydanych zaleceniach wskazano na potrzebę nadania odpowiednim funkcjonariuszom i pracownikom Wydziału Kadr upoważnienia do przetwarzania danych osobowych przetwarzanych poza zbiorami danych osobowych w zakresie niezbędnym do realizacji zadań służbowych. W ramach sprawdzenia dokonano kontroli zbiorów wymienionych w pkt 3 ppkt 1 sprawozdania, tj. „Centralna Baza Danych SG KADRY”, „Akta osobowe funkcjonariuszy i pracowników CSSG” oraz „Rejestr zaświadczeń i oświadczeń”.

W trakcie czynności kontrolnych Zastępca Naczelnika Wydziału Kadr [REDAKTOWANE] przedłożył zespołowi kontrolnemu informację<sup>37</sup> o prowadzonych w Wydziale Kadr rejestrach, książkach i ewidencjach ze wskazaniem jakie informacje zawierają poszczególne dokumenty. Z przedłożonej informacji wynika, że w Wydziale Kadr prowadzone są następujące dokumenty, zawierające dane osobowe:

- „Rejestr akt osobowych pracowników”,
- „Rejestr akt osobowych funkcjonariuszy SG”,
- „Roczne karty ewidencji obecności za rok ...”.

<sup>31</sup> dowód, akta kontroli – karty nr 135-136.

<sup>32</sup> dowód, akta kontroli – karty nr 101-109.

<sup>33</sup> dowód, akta kontroli – karty nr 101-109.

<sup>34</sup> dowód, akta kontroli – karty nr 137-143.

<sup>35</sup> dowód, akta kontroli – karty nr 144-151.

<sup>36</sup> dowód, akta kontroli – karty nr 152-158.

<sup>37</sup> dowód, akta kontroli – karty nr 159-161.

- „Emerytury i renty. Rejestr wniosków emerytalnych funkcjonariuszy CSSG”,
- „Tabela Ruchu Stanu Osobowego”.

Dokonane ustalenia wskazują ponadto, że dane osobowe zawierają również akta postępowań dyscyplinarnych, na podstawie których w Wydziale Kadr prowadzone są:

- „Ewidencja postępowań dyscyplinarnych i wyjaśniających”,
- „Ewidencja postanowień dyscyplinarnych”.

Z dokonanej przez zespół kontrolny analizy zapisów „Wykazu zbiorów danych osobowych przetwarzanych w CSSG” wynika, że w Wydziale Kadr prowadzone są następujące zbiory danych osobowych: „Akta osobowe funkcjonariuszy i pracowników”, „Centralna Baza Danych SG KADRY (CBD SG KADRY)”, „Ewidencja kandydatów do służby i pracy”, „Książka obsady etatowej”, „Rejestr zaświadczeń i oświadczeń”.

W odniesieniu do powyższego wskazać należy, że dla danych osobowych w zakresie emerytur i rent oraz postępowań dyscyplinarnych nie zostały utworzone zbiory danych osobowych. Wobec powyższego, zasadnym jest rozważenie możliwości utworzenia zbiorów danych osobowych dla w/w danych, ewentualnie utworzenie podzbioru dla w/w danych, co powinno nastąpić w porozumieniu z Naczelnikiem Wydziału Kadr CSSG.

W toku kontroli zespół kontrolny stwierdził ponadto, na podstawie analizy zapisów „Szczegółowych zakresów obowiązków i uprawnień” funkcjonariuszy i pracowników Wydziału Kadr<sup>38</sup> oraz wyjaśnień złożonych w dniu 25 maja 2017 r. przez Zastępcę Naczelnika Wydziału Kadr<sup>39</sup>, że osoby z Wydziału Kadr przygotowują projekty rozkazów o wyróżnieniu funkcjonariuszy skierowanych do CSSG na szkolenie. Sporządzenie przedmiotowej dokumentacji związane jest z przetwarzaniem danych osobowych słuchaczy CSSG. Powyższe wymaga nadania upoważnienia do przetwarzania danych osobowych w zbiorze „Rejestr słuchaczy”. Jak ustalono osoby opracowujące projekty przedmiotowych rozkazów nie posiadają upoważnienia do przedmiotowego zbioru danych osobowych<sup>40</sup>, co powinno być poddane korekcie w porozumieniu z Naczelnikiem Wydziału Kadr CSSG.

Odnośnie realizacji obowiązku dotyczącego opiniowania wniosków, dotyczących tworzenia, zmiany struktury lub zaprzestania przetwarzania danych osobowych w zbiorze danych ██████████ w wyjaśnieniach z dnia 16 maja 2017 r.<sup>41</sup> wskazał, że w większości przypadków wnioski o utworzenie, zmianę lub zaprzestanie przetwarzania danych osobowych, składane są przez kierowników komórek organizacyjnych do ADO za jego pośrednictwem. W takich przypadkach analizuje on zasadność utworzenia zbioru i podstawy prawne utworzenia zbioru, niejednokrotnie prowadząc konsultacje z Biurem Ochrony Informacji KGSG.

W zakresie realizacji procedur związanych z nadawaniem upoważnień do przetwarzania danych osobowych przez Komendanta CSSG Kierownik SSOI, w złożonych w dniu 16 maja 2017 r. wyjaśnieniach<sup>42</sup> stwierdził, że upoważnienia w większości przypadków nadawane są na wniosek kierowników komórek organizacyjnych. Zdarzają się przypadki, że nadawane one są bez wniosku, bądź wnioskują inne osoby widzące potrzebę upoważnienia osób do danego zbioru, co ma miejsce najczęściej w przypadku powoływania wszelkiego rodzaju

<sup>38</sup> dowód, akta kontroli – karty nr 162-167.

<sup>39</sup> dowód, akta kontroli – karta nr 169.

<sup>40</sup> dowód, akta kontroli – karty nr 170-174, 179-182.

<sup>41</sup> dowód, akta kontroli – karty nr 101-109.

<sup>42</sup> dowód, akta kontroli – karty nr 101-109.

komisji lub zespołów przez Komendanta CSSG. Upoważnienia są w takich sytuacjach nadawane na konkretny okres oraz ograniczone do niezbędnego zakresu danych. Przed wydaniem upoważnienia do przetwarzania danych osobowych (z wnioskiem, czy bez) zasadność wydania upoważnienia jest na bieżąco analizowana przez ABI przed przedstawieniem ADO do podpisu.

Odnosnie realizacji obowiązku opracowywania planu sprawdzeń, o którym mowa w rozporządzeniu *w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji*<sup>43</sup> [redacted] do wyjaśnień z dnia 16 maja 2017 r.<sup>44</sup> załączył opracowany na 2016 r. plan sprawdzeń. W przedmiotowych wyjaśnieniach stwierdził, że w 2017 r. nie jest jeszcze sporządzony plan sprawdzeń, gdyż po głębokiej analizie 2016 r. stwierdził, że nie ma potrzeby sporządzania takiego planu na cały rok. Sprawdzenia będą realizowane na bieżąco w miarę potrzeb i w miejscach wymagających sprawdzenia, a nie w z góry zamierzonych komórkach organizacyjnych. Przy planowaniu sprawdzeń będą zachowane terminy zgodnie z obowiązującymi przepisami.

W odniesieniu do powyższego wskazać należy, że zgodnie z § 3 ust 2 pkt 1 i 2. rozporządzenia w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych są przeprowadzane w trybie sprawdzenia planowego i doraźnego. Zgodnie z § 3 ust 5 w/w rozporządzenia plan sprawdzeń jest przygotowywany przez ABI na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiany administratorowi danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Powyższe oznacza, że plan sprawdzeń powinien być sporządzany obligatoryjnie, niezależnie od stanowiska ABI. Jeżeli zdaniem ABI nie ma potrzeby sporządzania planu sprawdzeń na okres 1 roku może on opracować plany sprawdzeń na okres jednego kwartału (co da 4 plany sprawdzeń w ciągu roku) lub jednego półrocza (co da 2 plany sprawdzeń w ciągu roku). Zaniechanie sporządzenia planu sprawdzeń za okres I kwartału 2017 r. stanowi naruszenie w/w obowiązku, co stanowi nieprawidłowość za którą odpowiedzialność ponosi [redacted] pełniący funkcję ABI.

W wyjaśnieniach z dnia 18 maja 2017 r. [redacted]<sup>45</sup> wskazał, że ZABI wykonuje powierzone zadania wyłącznie podczas nieobecności Kierownika SSOI. W chwili obecnej [redacted], w ocenie Kierownika SSOI, ma tak obszerny zakres obowiązków służbowych, że nie powierzono jej na stałe dodatkowych zadań związanych z realizacją funkcji ZABI.

Powyższy obszar kontroli zespół kontrolny ocenił pozytywnie z uchybieniami.

<sup>43</sup> Dz. U. z 2015 r. poz. 745, zwane dalej rozporządzeniem *w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji*.

<sup>44</sup> dowód, akta kontroli – karty nr 101-109.

<sup>45</sup> dowód, akta kontroli – karty nr 86-88.

3. Prawidłowość realizacji przez ABZ zadań określonych w Decyzji Nr 18 Komendanta CSSG.

Administratorem bezpieczeństwa zbioru wyznaczonym w drodze rozkazu dziennego Komendanta CSSG została [REDAKTOWANE]. Zadania ABZ zostały określone w § 17 Polityki bezpieczeństwa.

Wśród zadań ABZ Polityka bezpieczeństwa wymienia m.in. przygotowywanie, przechowywanie i rejestrowanie upoważnień do przetwarzania danych osobowych. W wyniku czynności kontrolnych zespół kontrolny ujawnił n/w uchybienia:

- nie odnotowanie daty wniosku o nadanie upoważnienia do przetwarzania danych osobowych;
- niejednolita praktyka w zakresie wskazywania w upoważnieniach do przetwarzania danych osobowych osoby wnioskującej o nadanie upoważnienia. Zgodnie z § 20 ust. 5 Polityki bezpieczeństwa za wystąpienie o nadanie/odwołanie upoważnienia odpowiedzialny jest bezpośredni przełożony. Zgodnie z wzorem upoważnienia do przetwarzania danych osobowych stanowiącym załącznik Nr 1 do Polityki bezpieczeństwa rubryki dotyczącej daty, imienia i nazwiska osoby występującej o nadanie/odwołanie upoważnienia nie wypełnia się w przypadku, gdy administrator danych lub inna upoważniona do tego osoba jest jednocześnie występującą o udzielenie upoważnienia. Zespół kontrolny, analizując zapisy wydanych upoważnień do przetwarzania danych osobowych, stwierdził że przedmiotowa rubryka w wielu przypadkach nie została wypełniona nawet w sytuacji, gdy osobą wnioskującą o nadanie upoważnienia nie był administrator danych ani upoważniona do tego osoba. Przypadki takiej praktyki zostały wskazane w „Zastrzeżeniach zespołu kontrolnego” z dnia 10 maja 2017 r.<sup>46</sup> i z dnia 17 maja 2017 r.<sup>47</sup>
- nie zaktualizowane nazwy podzbiorów w zbiorze „Dokumentacja ochrony obiektów” - podzbiory „Książka ewidencji przepustek i kart dostępu (stałych i okresowych) oraz przepustek samochodowych – kadra i pracownicy oraz słuchacze CSSG” i „Rejestr wydanych kart do depozytora kluczy” nie są wymienione jako zbiory ani podzbiory w arkuszu wykazu zbiorów danych przetwarzanych w CSSG, co prowadzi do wniosku, że upoważnienia nadane są do nieistniejących podzbiorów.

Powyżej wskazane uchybienie zostało skorygowane w trakcie czynności kontrolnych.

- błędne oznaczenie nazwy zbioru „Ewidencja osób przeszkolonych w zakresie ochrony danych osobowych/Rejestr wydanych zaświadczeń” i podzbioru „Lista obecności na szkoleniu” w upoważnieniu do przetwarzania danych osobowych nadanemu [REDAKTOWANE]. Faktycznie w/w zbiory są podzbiorymi zbioru „Szkolenia SSOI CSSG”. Pomimo tego, że w „Arkuszu Wykazu zbiorów danych przetwarzanych w CSSG” zawarto klauzulę informującą o tym, że upoważnienia do przetwarzania danych osobowych zawierające poprzednią nazwę zbioru danych zachowują ważność przez okres, na który zostały nadane, w analizowanej sytuacji zespół kontrolny, z uwagi na to, że nie ma możliwości przeprowadzenia ustalenia jakie podzbiory wchodziły w skład zbioru „Ewidencja osób przeszkolonych w zakresie ochrony danych osobowych/Rejestr wydanych zaświadczeń”, nie ma możliwości zweryfikowania zakresu udzielonego upoważnienia. W związku z powyższym, w ocenie zespołu kontrolnego, Kierownik SSOI powinien

<sup>46</sup> dowód, akta kontroli – karty nr 96-100.

<sup>47</sup> dowód, akta kontroli – karta nr 85.

zaktualizować wszystkie nadane upoważnienia pod względem aktualnych nazw zbiorów danych. Tym bardziej, że w wyjaśnienia złożonych w dniu 16 maja 2017 r. [REDAKTOWANE]

[REDAKTOWANE]<sup>48</sup> oświadczył, że „(...) wszelkie zmiany upoważnień będą dokonywane przy sprawdzeniach z zakresu ochrony danych osobowych w komórkach organizacyjnych CSSG.”

- w przypadku zbioru „Rejestr zaświadczeń i oświadczeń” nadawane były upoważnienia do nieistniejącego podzbioru tj. „Rejestr zaświadczeń i oświadczeń pracowników CSSG”.

- upoważnienie do zbioru „Bezpieczeństwo i higiena pracy”, podzbiory: „Postępowanie powypadkowe funkcjonariuszy”, „Postępowanie powypadkowe pracowników” zostało nadane Zastępcy Naczelnika Wydziału Kadr – [REDAKTOWANE]

z dniem 28 kwietnia 2017 r. (w trakcie czynności kontrolnych)<sup>49</sup> podczas, gdy od dnia 17 kwietnia 2015 r. decyzją nr 16 Komendanta CSSG z dnia 17 kwietnia 2015 r. wyznaczony został do komisji powypadkowej i w okresie objętym kontrolą faktycznie pełnił funkcję członka komisji powypadkowej, co wynika z Rozkazów dziennych Komendanta CSSG<sup>50</sup>.

- w przypadku zbioru „Archiwum SG” osobą wnioskującą o nadanie upoważnienia [REDAKTOWANE] jest Komendant CSSG, brak jest wskazania administratora danych w sytuacji, gdy u innych funkcjonariuszy CSSG (np. u [REDAKTOWANE]) jako osoba wnioskująca o nadanie upoważnienia występuje Kierownik SSOI, a jako administrator danych Komendant CSSG.

- nadane [REDAKTOWANE] upoważnienie do zbioru „Akta osobowe” podzbiór „Akta osobowe pracowników cywilnych” w sytuacji, gdy w ZWFiDS nie ma pracowników cywilnych. Zgodnie z § 20 ust. 4 Polityki bezpieczeństwa upoważnienie do przetwarzania danych nadaje się osobie, która w ramach realizowanych zadań służbowych przetwarza dane osobowe. Proponowany zakres uprawnień oraz nazwę zbiorów danych, do których osoba ma otrzymać upoważnienie i czas, na jaki ma być ono udzielone określa się na podstawie analizy zakresu obowiązków i uprawnień danej osoby. Skoro w ZWFiDS nie są zatrudnieni pracownicy cywilni nadane Kierownikowi ZWFiDS upoważnienie w w/w zakresie jest niezasadne.

- [REDAKTOWANE] raz nadane jest upoważnienie do zbioru „Rejestr słuchaczy”, podzbiór „Lista uczestników kursu/szkolenia” (z dnia 29 lutego 2012 r.), i po raz kolejny nadane jest upoważnienie do całego zbioru „Rejestr słuchaczy” (z dnia 11 lutego 2013 r.). W wyjaśnieniach złożonych w dniu 16 maja 2017 r. [REDAKTOWANE] wskazał, że pierwotnie nadane upoważnienie okazało się niewystarczające. W związku ze zwiększeniem zadań służbowych w/w nadano upoważnienie do całego zbioru. W ocenie zespołu kontrolnego nadanie upoważnienia do całego zbioru powinno skutkować odwołaniem wcześniej nadanego upoważnienia do jednego z podzbiorów.

W wyniku analizy upoważnień do przetwarzania danych osobowych zespół kontrolny ustalił, że w przeważającej części przypadków o nadanie upoważnienia do przetwarzania danych w określonych zbiorach lub podzbiorach występują kierownicy komórek organizacyjnych, których podpisy (w części przypadków pieczętunki i podpisy) widnieją w rubryce „data, imię i nazwisko lub pieczętunka imienna oraz podpis przełożonego (osoby wnioskującej)”. Treść w/w rubryki odzwierciedla zapis zawarty w § 20 ust. 5 Polityki bezpieczeństwa, zgodnie z którym za wystąpienie o nadanie/odwołanie upoważnienia

<sup>48</sup> dowód, akta kontroli – karty nr 101-109.

<sup>49</sup> dowód, akta kontroli – karty nr 126-130.

<sup>50</sup> dowód, akta kontroli – karty nr 185-198.

odpowiedzialny jest bezpośredni przełożony. Tymczasem wskazana powyżej praktyka, polegająca na występowaniu o nadanie upoważnienia przez kierowników komórek organizacyjnych, nie znajduje żadnego uzasadnienia w obowiązujących przepisach, zgodnie z którymi wystąpienie o nadanie upoważnienia leży w kompetencjach bezpośrednich przełożonych. Powyższe stanowi uchybienie, za które odpowiedzialność ponoszą [REDAKTOWANE] jako ABI odpowiedzialny za realizację procedur związanych z nadawaniem upoważnień do przetwarzania danych osobowych oraz [REDAKTOWANE] jako ABZ odpowiedzialny za przygotowywanie, przechowywanie i rejestrowanie upoważnień do przetwarzania danych osobowych.

Obok zbiorów danych osobowych, których administratorem jest Komendant CSSG, przetwarzane są także dane, których administratorem jest Komendant Główny SG, w których zgromadzone dane są powierzone do przetwarzania Komendantowi CSSG. Do zbiorów danych administrowanych przez Komendanta Głównego SG należą następujące zbiory danych: „CBD SG Kadry”, „Rejestr skarg i wniosków”, „Wykaz przedmiotów przekazanych Komendzie Głównej SG na mocy prawomocnych orzeczeń o ich przypadku”, „Centralna Baza danych SG System Wspomagania Kierowania (CBD SG SWK)”, „Archiwum SG” oraz „Rejestr przyjęć interesantów w sprawach skarg i wniosków”. Upoważnienia do przetwarzania danych osobowych zgromadzonych w w/w zbiorach może nadawać wyłącznie Komendant CSSG, co wynika z treści § 16 ust. 2 pkt 11 Polityki bezpieczeństwa, zgodnie z którym ABI nadaje i odwołuje, w imieniu Komendanta CSSG, upoważnienia do przetwarzania danych osobowych, których administratorem jest Komendant CSSG. *A contrario* ABI nie może nadać upoważnienia do przetwarzania danych osobowych zgromadzonych w zbiorze, którego administratorem jest Komendant Główny SG. W toku przeprowadzonej kontroli zespół kontrolny ujawnił przypadek, w którym upoważnienie do przetwarzania danych osobowych zgromadzonych w zbiorach administrowanych przez Komendanta Głównego SG nadał [REDAKTOWANE] pełniący funkcję ABI. Dotyczy to nadania upoważnienia do przetwarzania danych osobowych w zbiorze „Rejestr skarg i wniosków” [REDAKTOWANE] z dnia 21 czerwca 2011 r. udzielone przez [REDAKTOWANE]. Powyższe stanowi nieprawidłowość za którą odpowiedzialność ponoszą [REDAKTOWANE] jako ABI odpowiedzialny za realizację procedur związanych z nadawaniem upoważnień do przetwarzania danych osobowych, jak również bezpośrednio odpowiedzialny za nadanie upoważnienia poza posiadanymi uprawnieniami oraz [REDAKTOWANE] jako ABZ odpowiedzialny za przygotowywanie, przechowywanie i rejestrowanie upoważnień do przetwarzania danych osobowych.

Poza upoważnieniami wydawanymi indywidualnie oznaczonym osobom ABZ wydaje także upoważnienia grupowe (zbiorowe) nadawane uczestnikom kursu/szkolenia. Jak wynika z wyjaśnień złożonych w dniu 24 maja 2017 r. przez [REDAKTOWANE]<sup>51</sup> opisano szczegółowo procedurę gromadzenia danych niezbędnych do nadania w/w upoważnienia oraz procedurę nadawania upoważnienia zbiorowego.

W toku prowadzonej kontroli [REDAKTOWANE] przedłożyła zespołowi kontrolnemu dokumenty w postaci „Ewidencji osób upoważnionych do przetwarzania danych osobowych/Rejestru nadanych upoważnień” (Nr Rtd 86/10/131/15)<sup>52</sup> oraz „Dziennik działań

<sup>51</sup> dowód, akta kontroli – karty nr 200-201.

<sup>52</sup> dowód, akta kontroli – karty nr 202-210.



administratora bezpieczeństwa zbiorów w CSSG” (Nr RWD 10 p. 5/14)<sup>53</sup> prowadzona na podstawie § 17 ust. 1 pkt 4 i 10 Polityki bezpieczeństwa. Zgodnie z treścią art. 39 uodo ewidencja osób upoważnionych do przetwarzania danych osobowych powinna zawierać imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym. Przedłożona przez [REDAKTOWANE] „Ewidencja osób upoważnionych do przetwarzania danych osobowych/Rejestr nadanych upoważnień” spełnia wskazane powyżej ustawowe wymogi lecz nie jest systematycznie uaktualniana. W przedłożonej „Ewidencji osób upoważnionych do przetwarzania danych osobowych/Rejestrze nadanych upoważnień” nie są bowiem odnotowywane zmiany w zakresach udzielonych upoważnień do przetwarzania danych osobowych np. w sytuacji, gdy dochodzi do rozszerzenia udzielonego upoważnienia lub częściowego odwołania upoważnienia. Ponadto zespół kontrolny ujawnił przypadki braku odnotowania udzielonych upoważnień. W związku z powyższym w/w ewidencja nie odzwierciedla aktualnego stanu i zakresu udzielonych upoważnień do przetwarzania danych osobowych. W w/w zakresie zapisy „Ewidencji osób upoważnionych do przetwarzania danych osobowych/Rejestru nadanych upoważnień” nie odpowiadają treści zawartej w „Dzienniku działań administratora bezpieczeństwa zbiorów w CSSG”. Jako przykład w/w rozbieżności można wskazać nadanie w dniu 27 kwietnia 2017 r. upoważnienia [REDAKTOWANE], [REDAKTOWANE] oraz [REDAKTOWANE] upoważnienia do przetwarzania danych w zbiorze „Akta osobowe – uwierzytelniony wyciąg z akt osobowych funkcjonariusza policji i kandydata do służby w ZPiK CSSG” podczas gdy w/w upoważnienie nie zostało odnotowane w „Ewidencji osób upoważnionych do przetwarzania danych osobowych/Rejestrze nadanych upoważnień”. Kolejnym przykładem jest nadanie w dniu 10 stycznia 2017 r. [REDAKTOWANE] upoważnienia do przetwarzania danych osobowych w zbiorze „Rejestr słuchaczy – dokumentacja słuchaczy przebywających na kursie/szkoleniu w CSSG”, które także nie zostało ujęte w „Ewidencji osób upoważnionych do przetwarzania danych osobowych/Rejestrze nadanych upoważnień”.

Powyższe stanowi uchybienie za które odpowiedzialność ponosi [REDAKTOWANE]

[REDAKTOWANE], która jest odpowiedzialna za rzetelne prowadzenie w/w dokumentów.

Do zadań ABZ wskazanych w § 17 ust. 1 pkt 5 Polityki bezpieczeństwa należy prowadzenie wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w CSSG. W toku kontroli zespół kontrolny dokonał analizy zapisów zawartych w w/w wykazie, co zostało opisane w pkt VII.1.

W wyniku przeprowadzonych czynności kontrolny zespół kontrolny ujawnił, nieprawidłową w jego ocenie, praktykę polegającą na dokonywaniu skreśleń w upoważnieniach do przetwarzania danych osobowych bez informowania o tym osoby upoważnionej. Powyższa praktyka, polegająca np. na wykreślaniu podzbiorów danych w celu rozszerzenia upoważnienia na dane przetwarzane w całym zbiorze, skutkuje nadaniu nowego upoważnienia w rozszerzonym zakresie bez wniosku osoby uprawnionej oraz bez poinformowania o powyższym osoby upoważnionej. Skreślenie podzbioru i pozostawienie upoważnienia do całego zbioru parafowane jest jedynie przez [REDAKTOWANE]<sup>54</sup>. Korekta błędów literowych dokonywana jest przez [REDAKTOWANE], która dokonuje

<sup>53</sup> dowód, akta kontroli – karty nr 211-219.

<sup>54</sup> Dowód, akta kontroli – karty 110-130.

parafowania naniesionych poprawek. W ocenie zespołu kontrolnego powyżej opisaną praktykę dotyczącą zmian zakresów udzielonych upoważnień uznać należy za niedopuszczalną. W pierwszej kolejności należy wskazać, że nadanie/odwołanie upoważnienia do przetwarzania danych osobowych następuje na wniosek bezpośredniego przełożonego (§ 20 ust. 5 Polityki bezpieczeństwa), którego w omawianej sytuacji brak. Po wtóre, w ujawnionych przypadkach o zmianie zakresu upoważnienia nie była zawiadamiana osoba upoważniona (brak podpisów osób upoważnionych z datą dokonania zmian w upoważnieniu). Powyższe stanowi nieprawidłowość, za którą odpowiedzialność ponoszą [REDAKTOWANE] jako ABI odpowiedzialny za realizację procedur związanych z nadawaniem upoważnień do przetwarzania danych osobowych oraz [REDAKTOWANE] odpowiedzialny za przygotowywanie, przechowywanie i rejestrowanie upoważnień do przetwarzania danych osobowych.

Zgodnie z § 17 ust. 1 pkt 8 Polityki bezpieczeństwa do zadań ABZ należy prowadzenie szkoleń z zakresu ochrony danych osobowych oraz bezpieczeństwa systemów informatycznych. Szkolenia z w/w zakresu realizowane są zarówno w stosunku do funkcjonariuszy jak i pracowników CSSG, a także w odniesieniu do słuchaczy rozpoczynających szkolenie podstawowe w CSSG. Przeprowadzone szkolenia podlegają obowiązkowemu odnotowaniu w ewidencji osób przeszkolonych. Zespół kontrolny dokonał analizy zapisów w „Ewidencji osób przeszkolonych w zakresie ochrony danych osobowych/Rejestr wydanych zaświadczeń” (Rtd Nr 86/10/138/14), która zawierała dane wskazane w § 20 ust. 10 Decyzji Nr 129 Komendanta Głównego SG. Zespół kontrolny dokonał sprawdzenia realizacji obowiązku przeszkolenia z w/w zakresu porównując zapisy zawarte w w/w ewidencji z listami słuchaczy szkoleń podstawowych trwających w okresie objętym kontrolą<sup>55</sup>. W wyniku powyższego stwierdzono, iż 100% słuchaczy szkolenia podstawowego zostało przeszkolonych w wymaganym zakresie. Ponadto, w wyjaśnieniach złożonych w dniu 16 maja 2017 r. [REDAKTOWANE]<sup>56</sup> wskazał, że na dzień dzisiejszy wszyscy funkcjonariusze i pracownicy przetwarzający w CSSG dane osobowe posiadają przeszkolenie z zakresu ochrony danych osobowych, co potwierdzone jest wydanymi im zaświadczeniami. W zakresie realizacji obowiązku przeprowadzania szkoleń z zakresu ochrony danych osobowych uchybień nie stwierdzono.

Powyższy obszar kontroli zespół kontrolny ocenił pozytywnie z nieprawidłowościami.

#### 4. Prawidłowość realizacji przez ATI zadań określonych w Decyzji Nr 18 Komendanta CSSG.

Zgodnie z § 14 Polityki bezpieczeństwa za zabezpieczenie danych osobowych w CSSG odpowiadają m.in. Administratorzy Systemu Teleinformatycznego (ATI), których wyznaczenie w myśl § 15 ust. 4 następuje na podstawie rozkazu dziennego Komendanta CSSG. Komendant CSSG Rozkazem dziennym<sup>57</sup> do pełnienia obowiązków ATI wyznaczył [REDAKTOWANE] i [REDAKTOWANE] – jako administratora „Rejestru słuchaczy”. Zgodnie z § 18 ust. 1 Polityki bezpieczeństwa ATI odpowiedzialny jest za prawidłowe i bezpieczne funkcjonowanie systemu informatycznego, w którym

<sup>55</sup> dowód, akta kontroli – karty nr 220-229.

<sup>56</sup> dowód, akta kontroli – karty nr 101-109.

<sup>57</sup> dowód, akta kontroli – karty nr 237-239.

przetwarzane są dane osobowe w CSSG lub w komórce organizacyjnej CSSG, w której został wyznaczony. Zadania ATI wskazane są w § 18 ust. 2 Polityki bezpieczeństwa.

W zakresie realizacji zadania polegającego na konfiguracji stanowisk komputerowych zgodnie z wymaganiami, instalacji i aktualizacji oprogramowania, w tym antywirusowego, w wyjaśnieniach z dnia 09 maja 2017 r. ██████████<sup>58</sup> stwierdził, że w zakresie konfiguracji stanowisk komputerowych informacje dostaje od administratorów W-MOSG, co daje możliwość uzyskania pełnej zgodności dla wszystkich stanowisk pracujących w sieci teleinformatycznej SG. W zakresie ochrony antywirusowej odpowiednie aplikacje są instalowane zdalnie przez przynależność komputera do AD, zaś aktualizacje są realizowane w trybie automatycznym podczas pracy użytkownika.

Co do zadania polegającego na utrzymywaniu w aktualności hasła administratora systemu informatycznego ██████████ w w/w wyjaśnieniach<sup>59</sup> wskazał, że administratorem systemu informatycznego, z którego korzysta CSSG jest W-MOSG, który zabezpiecza funkcjonowanie CSSG, natomiast on sam jest tylko administratorem lokalnych stacji użytkowników i w tym przypadku nie ma potrzeby deponowania hasła ATI jako administratora. Poza tym nie istnieje ryzyko utraty tego hasła, ponieważ w razie zapomnienia, korzystając z usługi maximo hasło zostanie zresetowane do ustawień początkowych z wymuszeniem zmiany hasła przy ponownym logowaniu. Podczas nieobecności ██████████ wszelkie sprawy administracyjne realizuje również W-MOSG, a niektóre problemy mogą zostać rozwiązane również poprzez system Service Desk (maximo). Ponadto ██████████ wskazał, że nie administruje żadnym autonomicznym systemem, by zapewnić dostęp do administrowania nim podczas jego nieobecności.

W zakresie przyjętych w CSSG rozwiązań, dotyczących zakładania, blokowania i zamykania kont użytkowników systemu informatycznego ██████████ w wyjaśnieniach z dnia 09 maja 2017 r.<sup>60</sup> wskazał, że po uzyskaniu informacji z kadr o posiadanym dla nowej osoby identyfikatorze (ID-user), korzystając z przyznanych mu uprawnień zakłada w AD obiekt nowego użytkownika wpisując odpowiednie dane i przydzielając go do odpowiedniej grupy. Analogiczną czynność mogą wykonać administratorzy W-MOSG, jak również obsługa (servicedesk) maximo. Natomiast w przypadku ubycia osoby realizowana jest operacja wyłączenia obiektu, związanego z danym użytkownikiem. Obiekt taki jest następnie w sposób automatyczny przenoszony do odpowiedniego kontenera w ramach CSSG, ponieważ uprawnienia ██████████ ograniczają się tylko do gałęzi odpowiadającej swojej jednostce organizacyjnej.

Przyjęte w CSSG rozwiązania w zakresie sporządzania i przechowywania kopii zapasowych lokalnych systemów informatycznych i zbiorów danych polegają na tym, że wykonywanie lokalnych kopii zapasowych użytkownika spoczywa na ██████████, a ponadto administratorzy W-MOSG przygotowali zasób sieciowy indywidualny dla każdego użytkownika w celu wykonywania ewentualnych kopii swoich danych. Realizacja backupu danych, przechowywanych na dyskach sieciowych spoczywa w zakresie W-MOSG, który dysponuje odpowiednią infrastrukturą.

Procedura nadawania oraz odbierania uprawnień do zbiorów danych polega na tym, że na wniosek przełożonego następuje wpis do upoważnienia dla danej osoby, gdzie jest

<sup>58</sup> dowód, akta kontroli – karty nr 232-233.

<sup>59</sup> dowód, akta kontroli – karty nr 232-233.

<sup>60</sup> dowód, akta kontroli – karty nr 232-233.

określony zbiór danych oraz zakres uprawnień dla danego użytkownika. Administrator właściwej bazy realizuje wówczas dostęp dla podanego ID-user, przypisując odpowiednie uprawnienia. W przypadku odbierania uprawnień na wniosek właściwego przełożonego jest realizowany stosowny wpis w upoważnieniu i wówczas administrator właściwej bazy blokuje dostęp dla podanego ID-user.

W wyjaśnieniach z dnia 09 maja 2017 r. ██████████<sup>61</sup> wskazał, że nie był informowany o ujawnionych w CSSG przypadkach naruszenia bezpieczeństwa przetwarzania danych osobowych, w związku z tym nie są mu znane jakiegokolwiek działania w tym zakresie. Natomiast co do otrzymywania informacji o spostrzeżonych nieprawidłowościach w działaniu systemu informatycznego wyjaśnił, że ewentualne zgłoszenia dotyczyły awarii systemu lokalnej stacji użytkownika w związku z uszkodzeniem, czy to systemu plików, czy też sprzętu. W zależności od rodzaju uszkodzenia realizowane było zgłoszenia na maximo i komputer był dostarczany na warsztat W-MOSG w celu oceny możliwości i opłacalności naprawy. W przypadku awarii systemów plików zwykle jest realizowana reinstalacja systemu od nowa z formatowaniem dysku w celu odświeżenia systemu plików. Odzyskiwanie ewentualnych danych realizują administratorzy W-MOSG, którzy posiadają odpowiednie narzędzia i interfejsy.

Odnośnie sprawowania nadzoru nad przekazywaniem przez użytkowników uszkodzonych informatycznych nośników danych osobowych do właściwej kancelarii w celu zniszczenia ██████████ wskazał, że przenośne nośniki danych do przechowywania danych osobowych powinny być zarejestrowane i dany użytkownik rozlicza się z nimi w kancelarii skąd były pobierane. Dalsze czynności realizuje już właściwa kancelaria. Natomiast co do realizacji szkoleń w zakresie bezpieczeństwa systemów informatycznych ██████████ wyjaśnił, że przy przekazywaniu pierwszego hasła dla użytkownika realizowane jest szkolenie w zakresie zasad bezpieczeństwa pracy w systemie teleinformatycznym CSSG.

Zespół kontrolny pozytywnie ocenił powyższy obszar kontroli.

#### 5. Realizacja obowiązku przeprowadzania szkoleń funkcjonariuszy i pracowników CSSG z zakresu ochrony danych osobowych w CSSG.

Zgodnie z § 17 ust. 1 pkt 8 Polityki bezpieczeństwa do zadań ABZ należy prowadzenie szkoleń z zakresu ochrony danych osobowych oraz bezpieczeństwa systemów informatycznych. Szkolenia z w/w zakresu realizowane są zarówno w stosunku do funkcjonariuszy jak i pracowników CSSG, a także w odniesieniu do słuchaczy rozpoczynających szkolenie podstawowe w CSSG. Przeprowadzone szkolenia podlegają obowiązkowemu odnotowaniu w ewidencji osób przeszkolonych. Zespół kontrolny dokonał analizy zapisów w „Ewidencji osób przeszkolonych w zakresie ochrony danych osobowych/Rejestr wydanych zaświadczeń” (Rtd Nr 86/10/138/14), która zawierała dane wskazane w § 20 ust. 10 Decyzji Nr 129 Komendanta Głównego SG. Zespół kontrolny dokonał sprawdzenia realizacji obowiązku przeszkolenia z w/w zakresu porównując zapisy zawarte w w/w ewidencji z listami słuchaczy szkoleń podstawowych trwających w okresie objętym kontrolą<sup>62</sup>. W wyniku powyższego stwierdzono, iż 100% słuchaczy szkolenia

<sup>61</sup> dowód, akta kontroli – karty nr 232-233.

<sup>62</sup> dowód, akta kontroli – karty nr 220-229.

podstawowego zostało przeszkolonych w wymaganym zakresie. Ponadto, w wyjaśnieniach złożonych w dniu 16 maja 2017 r. ██████████<sup>63</sup> wskazał, że na dzień dzisiejszy wszyscy funkcjonariusze i pracownicy przetwarzający w CSSG dane osobowe posiadają przeszkolenie z zakresu ochrony danych osobowych, co potwierdzone jest wydanymi im zaświadczeniami. W zakresie realizacji obowiązku przeprowadzania szkoleń z zakresu ochrony danych osobowych uchybień nie stwierdzono.

Zespół kontrolny pozytywnie ocenił powyższy obszar kontroli.

6. Realizacja wymagań w zakresie przetwarzania danych osobowych, określonych w obowiązujących przepisach, dotyczących ochrony danych osobowych.

Wymagania w zakresie przetwarzania danych osobowych określone zostały w rozdziale 4 Polityki bezpieczeństwa (§ 20 i 21).

Zgodnie z treścią § 20 ust. 3 Polityki bezpieczeństwa do przetwarzania danych osobowych mogą być dopuszczone osoby, które spełniają łącznie następujące warunki: realizują zadania służbowe wymagające przetwarzania danych osobowych, odbyły szkolenie z zakresu ochrony danych osobowych oraz posiadają upoważnienie do przetwarzania danych osobowych.

Część ujawnionych uchybień dotyczących procedur nadawania upoważnień do przetwarzania danych osobowych została szczegółowo opisana we wcześniejszej części projektu wystąpienia pokontrolnego.

Dokonując analizy wydanych upoważnień do przetwarzania danych osobowych zespół kontrolny stwierdził, że:

- ██████████ nie posiada upoważnienia do przetwarzania danych osobowych zgromadzonych w zbiorze „Poświadczenia bezpieczeństwa”<sup>64</sup> w sytuacji, gdy zgodnie z pkt 4 Szczegółowego zakresu obowiązków i uprawnień Specjalisty ds. bezpieczeństwa dokumentacji SSOI w/w funkcjonariusz prowadzi rejestr wydanych poświadczeń bezpieczeństwa i wydanych upoważnień uprawniających do dostępu do informacji niejawnych o klauzuli „zastrzeżone” oraz na bieżąco informuje Wydział Kadr o zmianie poświadczenia bezpieczeństwa funkcjonariuszy i pracowników Centrum<sup>65</sup>.
- ██████████ nie posiada upoważnienia do przetwarzania danych osobowych zgromadzonych w zbiorze „Poświadczenia bezpieczeństwa” w sytuacji, gdy podlegli mu funkcjonariusze i pracownicy zgodnie z treścią Szczegółowych zakresów obowiązków i uprawnień prowadzą rejestr wydanych poświadczeń bezpieczeństwa i wydanych upoważnień uprawniających do dostępu do informacji niejawnych o klauzuli „zastrzeżone” oraz na bieżąco informują Wydział Kadr o zmianie poświadczenia bezpieczeństwa funkcjonariuszy i pracowników Centrum a ponadto, zgodnie z „Arkuszem wykazu zbiorów danych przetwarzanych w CSSG” zbiór „Poświadczenia bezpieczeństwa” jest prowadzony przez SSOI.
- ██████████ nie posiada upoważnienia do przetwarzania danych osobowych zgromadzonych w zbiorze „Oświadczenia majątkowe” podzbiór „Teczki oświadczeń majątkowych” w sytuacji, gdy zgodnie z pkt 7 Szczegółowego zakresu

<sup>63</sup> dowód, akta kontroli – karty nr 101-109.

<sup>64</sup> dowód, akta kontroli – karty nr 255-257.

<sup>65</sup> dowód, akta kontroli – karta nr 259.

obowiązków i uprawnień Specjalisty ds. bezpieczeństwa dokumentacji SSOI w/w funkcjonariusz prowadzi ewidencję i dokonuje analizy danych zawartych w oświadczeniach majątkowych funkcjonariuszy i pracowników Centrum Szkolenia Straży Granicznej zgodnie z obowiązującymi przepisami w tym zakresie i wydanym upoważnieniem. Zgodnie z treścią upoważnienia do przetwarzania danych osobowych [REDAKTION] upoważniony został do przetwarzania danych osobowych zawartych wyłącznie w podzbiorze „Rejestr teczek oświadczeń majątkowych”.

- [REDAKTION] nie posiada upoważnienia do przetwarzania danych osobowych zgromadzonych w zbiorze „Oświadczenia majątkowe” podzbiór „Teczki oświadczeń majątkowych” w sytuacji, gdy zgodnie z pkt 9 Szczegółowego zakresu obowiązków i uprawnień Kierownika SSOI nadzoruje on proces analizy oświadczeń o stanie majątkowym funkcjonariuszy i pracowników CSSG składanych Komendantowi CSSG. Zgodnie z treścią upoważnienia do przetwarzania danych osobowych [REDAKTION] upoważniony został do przetwarzania danych osobowych zawartych wyłącznie w podzbiorze „Rejestr teczek oświadczeń majątkowych”.

- [REDAKTION] nie posiada upoważnienia do przetwarzania danych osobowych zgromadzonych w zbiorze „Poświadczenia bezpieczeństwa” w sytuacji, gdy zgodnie z pkt 4 Szczegółowego zakresu obowiązków i uprawnień starszego inspektora SSOI w/w pracownik prowadzi rejestr wydanych poświadczeń bezpieczeństwa i wydanych upoważnień uprawniających do dostępu do informacji niejawnych o klauzuli „zastrzeżone” oraz na bieżąco informuje Wydział Kadr o zmianie poświadczenia bezpieczeństwa funkcjonariuszy i pracowników Centrum.

- [REDAKTION] – Pełnomocnik Komendanta CSSG do spraw Ochrony Praw Człowieka i Równego Traktowania nie posiada upoważnienia do przetwarzania danych osobowych zgromadzonych w zbiorze „Ewidencja kandydatów do służby przygotowawczej i pracy” w ramach którego przetwarzane są dane osobowe w zakresie związanym z wyznaczeniem jej do zespołu do przeprowadzania wstępnych rozmów kwalifikacyjnych z kandydatami do służby w CSSG (Decyzja Komendanta CSSG Nr 34 z dnia 27 kwietnia 2016 r. zmieniająca decyzję w sprawie wyznaczenia zespołu do przeprowadzania wstępnych rozmów kwalifikacyjnych z kandydatami do służby w CSSG<sup>66</sup>).

- [REDAKTION] nie posiada upoważnienia do zbioru „Rejestr słuchaczy” podzbiór „Rejestr słuchaczy” w ramach którego przetwarzane są dane osobowe dotyczące wyników nauczania<sup>67</sup>, w sytuacji gdy zgodnie ze Szczegółowym zakresem obowiązków i uprawnień Samodzielnego Referenta WliOD w/w pracownik m.in. zapewnia obsługę ewidencji wyników szkolenia, w tym opracowanie zbiorczych zestawień wyników uzyskiwanych w trakcie szkolenia.

- pracownicy Kancelarii Tajnej SSOI CSSG posiadają upoważnienie do przetwarzania danych osobowych wyłącznie w zbiorze „Archiwum SG”<sup>68</sup>, natomiast [REDAKTION] nie posiada upoważnienia do przetwarzania jakichkolwiek danych osobowych, podczas gdy w/w osoby, zgodnie ze Szczegółowymi zakresami obowiązków i uprawnień, wykonują czynności

<sup>66</sup> dowód, akta kontroli – karty nr 234-236.

<sup>67</sup> dowód, akta kontroli – karta nr 113.

<sup>68</sup> dowód, akta kontroli – karty nr 263, 264.

kancelaryjne w zakresie obiegu dokumentów jawnych zgodnie z wydanym upoważnieniem do wykonywania czynności kancelaryjnych<sup>69</sup>.

W wyjaśnieniach złożonych w dniu 25 maja 2017 r. przez ██████████<sup>70</sup> wskazano, co następuje:

- odnośnie braku upoważnień do przetwarzania danych osobowych w zbiorze „Poświadczenia bezpieczeństwa” Kierownik SSOI stwierdził, że dane osobowe w zbiorze „Poświadczenia bezpieczeństwa w okresie objętym kontrolą przetwarzali: ██████████, ██████████  
██████████ oraz ██████████. Ponadto stwierdził, że zakres danych w tym zbiorze mieścił się w zbiorach dotyczących postępowań sprawdzających. Po zmianie wykazu zbiorów danych osobowych przetwarzanych w CSSG w dniu 27 czerwca 2013 r., gdzie powstały dwa oddzielne zbiory danych, tj. postępowania sprawdzające i poświadczenia bezpieczeństwa powinien wnioskować o nadanie odrębnego upoważnienia. ██████████ zaznaczył jednak, że zbiór „Poświadczenia bezpieczeństwa” dotyczy wyłącznie wykazu poświadczeń bezpieczeństwa, który zgodnie z ustawą powinien prowadzić Pełnomocnik ochrony. W trakcie prowadzonej kontroli nadano ██████████  
██████████ i ██████████ upoważnienia do przetwarzania danych osobowych w zbiorze „Poświadczenia bezpieczeństwa”.

- odnośnie braku upoważnień do przetwarzania danych osobowych w zbiorze „Oświadczenia majątkowe” Kierownik SSOI stwierdził, że w okresie objętym kontrolą dane osobowe w przedmiotowym zbiorze przetwarzali: ██████████, ██████████  
██████████ oraz ██████████. W trakcie dokonywania wpisu w blankiecie upoważnienia został popełniony błąd. Po zmianach wykazu zbiorów w rubryce „Nazwa zbioru” nie został wykreślony podzbiór „Rejestr teczek oświadczeń majątkowych”. Przedmiotowy błąd został naprawiony w trakcie czynności kontrolnych w dniu 11 maja 2017 r. poprzez skreślenie nadpisanego tekstu. W wyjaśnieniach złożonych w dniu 25 maja 2017 r. ██████████<sup>71</sup> wskazał, że ABZ powinien nanieść techniczną zmianę wykreślając podzbiór, dopisać podzbiór do upoważnienia do przetwarzania danych osobowych lub nadać nowe upoważnienie do całego zbioru.

W trakcie czynności kontrolnych zespół kontrolny stwierdził ponadto, że przedłożone do kontroli przez Kierownika SSOI upoważnienia ██████████ (Nr 95/U/15 z dnia 06.11.2015 r.), ██████████ (Nr 96/U/15 z dnia 06.11.2015 r.) oraz ██████████ (Nr 97/U/15 z dnia 06.11.2015 r.)<sup>72</sup> do dokonywania analizy danych zawartych w oświadczeniach o stanie majątkowym są nieważne, gdyż zawierały nieaktualne podstawy prawne ich wydania. W trakcie czynności kontrolnych ██████████ przedłożył zespołowi kontrolnemu nowe upoważnienia (Nr 12/17, Nr 13/17 i Nr 14/17)<sup>73</sup>, podpisane przez Komendanta CSSG w dniu 19.05.2017 r. W odniesieniu do powyższego stwierdzić należy, że dokonywanie przez w/w osoby analizy danych zawartych w oświadczeniach o stanie majątkowym stanowi nieprawidłowość, za którą odpowiedzialność ponosi Kierownik SSOI, jako osoba odpowiedzialna za zapewnienie sobie i podległej kadrze aktualnych upoważnień do wykonywania na ich podstawie czynności

<sup>69</sup> dowód, akta kontroli – karty nr 265-267.

<sup>70</sup> dowód, akta kontroli – karty nr 90-93.

<sup>71</sup> dowód, akta kontroli – karty nr 90-93.

<sup>72</sup> dowód, akta kontroli – karty nr 272-274.

<sup>73</sup> dowód, akta kontroli – karty nr 275-277.

służbowych oraz [REDAKTOWANE] i [REDAKTOWANE] poprzez realizację obowiązków służbowych na podstawie nieaktualnych upoważnień.

- odnośnie braku upoważnień do przetwarzania danych osobowych w zbiorze „Ewidencja kandydatów do służby przygotowawczej i pracy” nadanego [REDAKTOWANE] Kierownik SSOI stwierdził, że do SSOI nie wpłynęły stosowne wnioski, w związku czym upoważnienie nie zostało nadane.

- odnośnie braku upoważnień do przetwarzania danych osobowych w zbiorze „Rejestr słuchaczy” podzbiór „Rejestr słuchaczy” nadanego [REDAKTOWANE] Kierownik SSOI w wyjaśnieniach z dnia 25 maja 2017 r.<sup>74</sup> stwierdził, że w/w osoba posiadała upoważnienie do przetwarzania danych osobowych w całym zbiorze „Rejestr słuchaczy”. Po dokonaniu wewnętrznego podziału zbioru na trzy podzbiory osoba przeprowadzająca podział dokonała odrębnego dopisku na blankiecie upoważnienia dopisując nazwy dwóch z trzech podzbiorów traktując wszystko jako trzy części składające się na omawiany zbiór, o czym, zdaniem Kierownika SSOI nawet nie było potrzeby informować [REDAKTOWANE], gdyż zmianie uległa struktura zbioru a nie zakres upoważnienia. Jak wskazano w dalszej części wyjaśnień, „ten zapis sprawia wrażenie ograniczenia upoważnienia” wyłącznie do dwóch z trzech podzbiorów co nie prowadzi do przetwarzania danych bez upoważnienia. Kierownik SSOI wskazał, że „inne podejście do przedmiotowej sprawy tworzyłoby niepotrzebne nadawanie i odbieranie upoważnień dla funkcjonariuszy i pracowników”. Kierownik SSOI poddaje w wątpliwość zasadność nadawania nowych upoważnień do przetwarzania danych osobowych po każdej zmianie w zakresie przetwarzania danych, ponieważ nie ma żadnego znaczenia dla funkcjonowania zbioru. W trakcie czynności kontrolnych w upoważnieniu [REDAKTOWANE] Kierownik SSOI wykreślił dwa podzbiory rozszerzając tym samym zakres upoważnienia do całego zbioru „Rejestr słuchaczy” obejmującego także dane dotyczące wyników nauczania<sup>75</sup>.

Zdaniem zespołu kontrolnego wskazane powyżej wyjaśnienia Kierownika SSOI nie zasługują na uwzględnienie. W pierwszej kolejności należy wskazać, że praktyka polegająca na nadawaniu lub odbieraniu upoważnień do przetwarzania danych osobowych poprzez dokonywanie odrębnych dopisków do formularza upoważnienia przez dopisywanie lub wykreślanie podzbiorów albo odręcznie wykonywaną modyfikację zakresu przetwarzanych danych, bez wniosku bezpośredniego przełożonego i zawiadomienia o dokonywanych zmianach osoby upoważnionej, jest całkowicie pozbawiona podstaw prawnych. Odnosząc się do opisywanego powyżej przypadku utworzenie w zbiorze „Rejestr słuchaczy” trzech podzbiorów i nadanie upoważnienia tylko do dwóch z nich, zdaniem zespołu kontrolnego nie tylko „sprawia wrażenie ograniczenia upoważnienia” lecz wprost to upoważnienie ogranicza tylko do wskazanych w upoważnieniu podzbiorów. Jeżeli na skutek podziału zbioru na podzbiory upoważnienie zostało nadane tylko do części nowoutworzonych podzbiorów to osoba upoważniona do części podzbiorów nie ma prawa przetwarzać danych osobowych w tych podziorach, na które nie rozciąga się posiadane przez nią upoważnienie. Ponadto wskazać należy, że powyżej opisana praktyka stosowana w SSOI skutkuje tym, że osoby upoważnione oraz ich bezpośredni przełożeni (jako wnioskujący o nadanie upoważnienia w pierwotnym zakresie) nie znają rzeczywistego zakresu udzielonych im upoważnień do zmodyfikowanych zbiorów.

<sup>74</sup> dowód, akta kontroli – karty nr 90-93.

<sup>75</sup> dowód, akta kontroli – karta 113.



Powyższe stanowi nieprawidłowość za którą odpowiedzialność ponosi [REDAKTOWANE] jako ABI odpowiedzialny za realizację procedur związanych z nadawaniem upoważnień do przetwarzania danych osobowych i [REDAKTOWANE] jako ABZ odpowiedzialny za przygotowywanie, przechowywanie i rejestrowanie upoważnień do przetwarzania danych osobowych.

Powyższy obszar kontroli zespół kontrolny ocenił pozytywnie z nieprawidłowościami.

7. Stosowanie środków technicznych i organizacyjnych, niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Stosowane w CSSG podczas przetwarzania danych osobowych środki techniczne i organizacyjne określa rozdział 6 Polityki bezpieczeństwa, wskazując na środki bezpieczeństwa w zakresie ochrony fizycznej oraz środki techniczne i organizacyjne dotyczące urządzeń i systemów informatycznych, służących do przetwarzania danych osobowych określone w odrębnych przepisach, w szczególności w rozporządzeniu w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. W wyjaśnieniach z dnia 22 maja 2017 r. [REDAKTOWANE] wskazał, iż mając powyższe na względzie w CSSG opracowana została dokumentacja przetwarzania danych osobowych spełniająca warunki określone w § 3, 4 i 5 powyższego rozporządzenia. Dokumentacja ta stanowi akta sprawy nr Rtd 11/17 „Podstawowe założenia polityki ochrony danych osobowych. Dokumentacja przetwarzania danych osobowych w CSSG”, w skład której wchodzi: decyzja nr 18 Komendanta CSSG, „Wykaz zbiorów danych osobowych przetwarzanych w CSSG” z dnia 12 maja 2016 r., „Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są zbiory danych osobowych” oraz „Rejestr zbiorów danych osobowych, którego wymóg prowadzenia narzuca art. 36a ust. 2 pkt 2 uodo. W w/w wyjaśnieniach [REDAKTOWANE] wskazał ponadto, że w związku z faktem, że obsługę logistyczno-finansową CSSG zapewnia Komendant W-MOSG administratorem systemu informatycznego użytkowanego w CSSG jest W-MOSG, który m.in. zapewnia zabezpieczenie systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. W-MOSG zapewnia też m.in. ochronę przed zagrożeniami płynącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. Środki techniczne i organizacyjne stosowane w CSSG określa ponadto „Plan ochrony informacji niejawnych CSSG, w tym w razie wprowadzenia stanu nadzwyczajnego”. Z wyjaśnień Kierownika SSOI wynika także, że wymóg odnotowywania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym dotyczy tylko systemów używanych do przetwarzania danych osobowych w zbiorach niejawnych, a takich systemów w CSSG nie ma.

Zespół kontrolny pozytywnie ocenił powyższy obszar kontroli.

<sup>76</sup> dowód, akta kontroli – karty nr 74-81.

<sup>77</sup> dowód, akta kontroli – karty nr 74-81.

8. Stosowanie „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w CSSG”.

„Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w CSSG” została określona w Załączniku Nr 2 do Decyzji Nr 18 Komendanta CSSG. W/w instrukcja zawiera ogólne procedury zarządzania systemami informatycznym oraz warunki i sposób postępowania przy wykorzystaniu systemów służących do przetwarzania danych osobowych w CSSG.

W wyjaśnieniach złożonych w dniu 22 maja 2017 r. Kierownik SSOI<sup>78</sup> wskazał, że w związku z tym, że obsługę logistyczno-finansową CSSG zapewnia Komendant W-MOSG administratorem systemu informatycznego użytkowanego w CSSG jest W-MOSG, który jest zobowiązany do zapewnienia m.in. zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz utrata danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. W-MOSG zapewnia też ochronę systemu przez zagrożeniami płynącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

Jak natomiast wynika z informacji złożonej w dniu 09 maja 2017 r. przez [REDAKTOWANE] – Specjalistę SOD WliOD<sup>79</sup>, który jednocześnie pełni funkcję ATI, administratorem systemu informatycznego z którego korzysta CSSG jest W-MOSG. W zakresie konfiguracji stanowisk komputerowych sposób konfiguracji jest określany przez administratorów W-MOSG, skutkiem czego uzyskana jest pełna zgodność dla wszystkich stanowisk pracujących w sieci teleinformatycznej SG. W wyjaśnieniach złożonych w dniu 23 maja 2017 r. [REDAKTOWANE]<sup>80</sup> wskazał, że w CSSG nie ma komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych. Jeżeli zachodzi konieczność przetwarzania danych osobowych na komputerze przenośnym istnieje możliwość zaszyfrowania całego dysku mechanizmem BitLocker, tak jak w przypadku nośników wymiennych. Jednocześnie zespołowi kontrolnemu został przedłożony „Dziennik pracy administratora teleinformatycznego zbiorów danych osobowych CSSG” (RWD Nr 15/1/17)<sup>81</sup>.

Przyjęte rozwiązania w zakresie realizacji zapisów zawartych w „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w CSSG” zostały szczegółowo opisane we wcześniejszej części projektu wystąpienia pokontrolnego.

Sposób zapewnienia ochrony danych osobowych przetwarzanych w CSSG w systemach informatycznych jest zgodny z zapisami zawartymi w w/w instrukcji.

Zespół kontrolny powyższy obszar kontroli ocenił pozytywnie.

Do ustaleń i oceny zawartych w projekcie wystąpienia pokontrolnego z kontroli zgodnej z rocznym planem kontroli, zrealizowanej w trybie zwykłym na temat „Sprawowanie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, przetwarzanych w Centrum Szkolenia Straży Granicznej.” (pismo nr CS-NK.0910.2.2017 z dnia 04.07.2017 r.) Kierownik SSOI [REDAKTOWANE] wniósł zastrzeżenia (pismo nr CS-OI.0910.1.2017

<sup>78</sup> dowód, akta kontroli – karty nr 74-81.

<sup>79</sup> dowód, akta kontroli – karty nr 232-233.

<sup>80</sup> dowód, akta kontroli – karta nr 269.

<sup>81</sup> dowód, akta kontroli – karty nr 278-279.

z dnia 07.07.2017 r.). Na podstawie § 29 ust. 1-3 wytycznych w związku z § 1 Decyzji nr 139 Komendanta Głównego Straży Granicznej z dnia 30 sierpnia 2012 r. w sprawie wprowadzenia do stosowania w Straży Granicznej wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach, obsługujących organy lub w jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych sporządzone zostało przez zespół kontrolny stanowisko dotyczące wniesionych przez Kierownika SSOI [REDAKTOWANE] zastrzeżeń do ustaleń i ocen, zawartych w projekcie wystąpienia pokontrolnego (pismo nr CS-NK.0910.2.2017 z dnia 12.07.2017 r.).

Po zapoznaniu się ze stanowiskiem zespołu kontrolnego w przedmiocie wniesionych przez Kierownika SSOI zastrzeżeń do projektu wystąpienia pokontrolnego, zastrzeżenia te należało uznać za bezzasadne i je oddalić.

### **VIII. Zalecenia i wnioski dotyczące usunięcia nieprawidłowości lub usprawnienia funkcjonowania podmiotu kontrolowanego:**

#### **1. Zalecenia:**

W związku z przeprowadzoną kontrolą i ustaleniami zawartymi w przedmiotowym wystąpieniu pokontrolnym, w celu usunięcia stwierdzonych uchybień i nieprawidłowości oraz w celu usprawnienia funkcjonowania podmiotu kontrolowanego, polecam:

- 1) omówić z podległą kadrą ujawnione w trakcie kontroli uchybienia i nieprawidłowości opisane w przedmiotowym wystąpieniu pokontrolnym,
- 2) w uzgodnieniu z kierownikami komórek organizacyjnych przeanalizować wszystkie nadane upoważnienia do przetwarzania danych osobowych pod kątem ich zakresów, zasadności nadania oraz nazw zbiorów danych osobowych i ich podzbiorów,
- 3) trwale wyeliminować praktykę polegającą na zmianie zakresów nadanych upoważnień przez dopisywanie podzbiorów lub ich wykreślanie w blankietach upoważnień,
- 4) zmianę zakresu upoważnienia realizować poprzez odwołanie upoważnienia i nadanie nowego z nowookreślonym zakresem,
- 5) zgodnie z „Polityką bezpieczeństwa” upoważnienia nadawać na wniosek bezpośrednich przełożonych osób, którym ma być nadane upoważnienie,
- 6) przestrzegać właściwości do nadawania upoważnień przez Komendanta CSSG do zbiorów danych osobowych, których administratorem jest Komendant Główny SG,
- 7) zainicjować zmianę „Polityki bezpieczeństwa” w zakresie skorygowania błędnego odesłania do osób funkcyjnych, zawartego w § 15 ust. 4,
- 8) dokonać uzgodnień z Naczelnikiem Wydziału Kadr w zakresie możliwości utworzenia zbiorów danych osobowych lub podzbiorów dla danych osobowych w zakresie postępowań dyscyplinarnych oraz emerytur i rent,
- 9) odnotowywać historię zmian dokonaną w „Wykazie zbiorów danych osobowych przetwarzanych w CSSG”,
- 10) w „Wykazie zbiorów danych osobowych przetwarzanych w CSSG” i w „Rejestrze zbiorów danych osobowych przetwarzanych w CSSG” skorygować nagłówki tabel poprzez wskazanie jako administratora zbiorów danych Komendanta CSSG,
- 11) zaktualizować „Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są zbiory danych osobowych”,

- 12) opracowywać plan sprawdzeń zgodnie z rozporządzeniem w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji,
- 13) na bieżąco aktualizować „Ewidencję osób upoważnionych do przetwarzania danych osobowych/Rejestr nadanych upoważnień”,
- 14) ustalenia kontroli zawarte w niniejszym wystąpieniu pokontrolnym wykorzystać w działalności służbowej w celu uniknięcia w przyszłości podobnych uchybień i nieprawidłowości.

Z uwagi na fakt nadania w trakcie czynności kontrolnych wymaganych upoważnień wniosku w tym zakresie nie formułowano.

2. Wnioski:

W związku z przeprowadzoną kontrolą i ustaleniami zawartymi w przedmiotowym wystąpieniu pokontrolnym, w celu usprawnienia funkcjonowania podmiotu kontrolowanego rozważyć:

- 1) zmianę „Polityki bezpieczeństwa” w zakresie:
  - rozszerzenia uprawnienia do występowania z wnioskiem o nadanie/odwołanie upoważnienia do przetwarzania danych osobowych także przez kierowników komórek organizacyjnych,
  - określenie w „Polityce bezpieczeństwa” formy występowania z wnioskiem o nadanie/odwołanie upoważnienia.

- IX. Informację o wykonaniu zaleceń i wykorzystaniu wniosków, a także o podjętych działaniach lub przyczynach ich niepodjęcia należy przedłożyć Komendantowi CSSG w terminie do dnia 30 września 2017 r.
- X. Zgodnie z § 34 wytycznych, stanowiących załącznik do Decyzji nr 65 Ministra Spraw Wewnętrznych z dnia 31 maja 2012 r. w sprawie wprowadzenia do stosowania wytycznych w zakresie zasad i trybu przeprowadzania kontroli w urzędach obsługujących organy lub w jednostkach organizacyjnych podległych lub nadzorowanych przez Ministra Spraw Wewnętrznych (Dz. Urz. MSW z 2012 r. poz. 43 z późn. zm.) *”Od wystąpienia pokontrolnego nie przysługują środki odwoławcze”*.
- XI. Wystąpienie pokontrolne sporządzono w dwóch jednobrzmiących egzemplarzach, z których jeden przeznaczony jest dla kierownika podmiotu kontrolowanego.
- XII. Fakt przeprowadzenia kontroli odnotowano w „Książce kontroli Centrum Szkolenia Straży Granicznej” zarejestrowanej w Samodzielnej Sekcji Ochrony Informacji CSSG, pod numerem wg opisu Rtd Nr 104/12, l.p. 2 z 2017 r., prowadzonej przez Referat Kontroli w Kierownictwie Centrum Szkolenia Straży Granicznej.

  
płk SG Roman LUBIŃSKI

.....  
stopień, imię i nazwisko oraz podpis zarządzającego kontrolę

Wykonano w 2 egzemplarzach:  
Egz. nr 1 – Kierownik SSOI  
Egz. nr 2 – a/a  
Wykonał: Katarzyna Pejda  
Nr tel.: 6643283  
Dnia: 14.07.2017 r.