

Warszawa, dnia 29 września 2011 r.

Sprawozdanie z pracy Zespołu doraźnego do spraw pozyskiwania danych telekomunikacyjnych.

Zespół doraźny do spraw pozyskiwania danych telekomunikacyjnych, zwany dalej Zespołem, powołany został decyzją Przewodniczącego Kolegium do Spraw Służb Specjalnych z dnia 8 marca 2011 r. Zadaniem Zespołu było wypracowanie stanowiska w sprawie zmian legislacyjnych dotyczących pozyskiwania przez uprawnione organy danych objętych tajemnicą telekomunikacyjną, a także przygotowanie propozycji tych zmian.

W dniu 22 czerwca 2011 r. Przewodniczący Kolegium wydał decyzję nowelizującą decyzję z dnia 8 marca 2011 r. w sprawie powołania Zespołu – rozszerzając tym samym zakres przedstawicieli organów i instytucji mogących uczestniczyć w posiedzeniach Zespołu. Od czerwca br. w pracach Zespołu wzięli udział także przedstawiciele Ministerstwa Infrastruktury oraz Urzędu Komunikacji Elektronicznej.

W skład Zespołu do spraw pozyskiwania danych telekomunikacyjnych weszli:

- Przewodniczący – Jacek Cichocki – Sekretarz Kolegium do Spraw Służb Specjalnych,
- Zastępca przewodniczącego – Tomasz Borkowski – Dyrektor Biura Kolegium do Spraw Służb Specjalnych,
- Sekretarz Zespołu – Robert Górecki – radca prawny KPRM w Biurze Kolegium do Spraw Służb Specjalnych,
- Prokurator Paweł Burzyński – Departament Legislacyjno – Prawny Ministerstwa Sprawiedliwości,
- Piotr Butrym – Zastępca Dyrektora Biura Informatyki i Telekomunikacji Ministerstwa Spraw Zagranicznych,
- płk Jarosław Chudek – Zastępca Szefa Oddziału Stacjonarnych Systemów Teleinformatycznych Zarządu Planowania Systemów Dowodzenia i Łączności – P6 Sztabu Generalnego Wojska Polskiego Ministerstwa Obrony Narodowej,

- Zbigniew Czucha – Naczelnik Wydziału Nadzoru i Koordynacji Służb Porządku Publicznego w Departamencie Nadzoru i Analiz MSWiA,
- Przemysław Czyż – Ministerstwo Spraw Zagranicznych,
- Łukasz Filipiak – Dyrektor Biura Prawnego Centralnego Biura Antykorupcyjnego,
- ppłk Marcin Godynicki – Zastępca Dyrektora Biura Techniki Operacyjnej Służby Kontrwywiadu Wojskowego,
- ppłk Jacek Grabowski – Starszy Specjalista Oddziału Stacjonarnych Systemów Teleinformatycznych Zarządu Planowania Systemów Dowodzenia i Łączności – P6 Sztabu Generalnego Wojska Polskiego Ministerstwo Obrony Narodowej,
- Maciej Groń – Zastępca Dyrektora Departamentu Społeczeństwa Informacyjnego Ministerstwa Spraw Wewnętrznych i Administracji,
- Rafał Gruszka – Ministerstwo Infrastruktury,
- Marek Jurkiewicz – Zastępca Dyrektora Departamentu Spraw Obronnych Urzędu Komunikacji Elektronicznej,
- por. Michał Kamiński – Ekspert w Biurze Prawnym Agencji Bezpieczeństwa Wewnętrznego,
- Marek Kostro – Wydział Bezpieczeństwa Publicznego Departamentu Bezpieczeństwa Pozamilitarnego Biura Bezpieczeństwa Narodowego,
- kpt. Artur Krzemiński – Służba Kontrwywiadu Wojskowego,
- por. SG Arkadiusz Matyjasik – Kierownik Samodzielnej Sekcji Przepisów Zarządu Operacyjno – Śledczego Komendy Głównej Straży Granicznej,
- płk Przemysław Michalak – Szef Oddziału Sieci Teleinformatycznych Departamentu Informatyki i Telekomunikacji Ministerstwa Obrony Narodowej,
- kpt. Jacek Mirgos – Naczelnik Samodzielnego Wydziału Prawnego Agencji Wywiadu,
- płk Mieczysław Misiuda – Służba Wywiadu Wojskowego,
- płk Kazimierz Mordaszewski – Dyrektor Biura Prawnego Agencji Bezpieczeństwa Wewnętrznego,
- Małgorzata Olszewska – Ministerstwo Infrastruktury,
- Jakub Pałka – Służba Wywiadu Wojskowego,
- Paweł Skowronek – Zastępca Dyrektora Departamentu Wywiadu Skarbowego Ministerstwa Finansów,
- Prokurator Marek Staszak – Zespół Kontroli Działań Operacyjnych Organów Ścigania Biura Prokuratora Generalnego,
- Anna Streżyńska – Prezes Urzędu Komunikacji Elektronicznej,
- Adam Szczepański – Dyrektor Biura Techniki Operacyjnej Centralnego Biura Antykorupcyjnego,
- nadinspektor Kazimierz Sz wajcowski – Pierwszy Zastępca Komendanta Głównego Policji,
- dyr Marek Ślizak – Komenda Główna Policji,
- Prokurator Beata Wiraszka – Bereza – Ministerstwo Sprawiedliwości,

- Prokurator Włodzimierz Wolny – Prokurator Prokuratury Generalnej,
- ppłk Rafał Wyżnikiewicz – Zarząd Dochodzeniowo – Śledczy Komendy Głównej Żandarmerii Wojskowej.

Zespół zebrał się na trzech posiedzeniach. Podczas pierwszego, które odbyło się w dniu 11 kwietnia 2011 r. określono zasady i harmonogram prac. Przewodniczący Zespołu przedstawił zasadnicze powody powołania tego gremium oraz cele jego pracy. Przypomniął, iż jesienią 2010 r. w mediach rozgorzała dyskusja dotycząca uregulowań prawnych i praktyki pozyskiwania przez uprawnione instytucje państwowe danych telekomunikacyjnych obejmujących rejestry połączeń (bilingi), ustalenia abonenckie i lokalizacyjne. Dyskusja ta stała się podstawą dla wystąpienia Rzecznika Praw Obywatelskich do Prezesa Rady Ministrów, w którym przedstawiono postulaty dotyczące ograniczenia zakresu przypadków, w których uprawnione służby pozyskują dane telekomunikacyjne, zastosowania zasady subsydiarności, niezwłocznego niszczenia danych, które nie zostały wykorzystane, ograniczenia możliwości pozyskiwania danych dziennikarzy i adwokatów oraz poddania pozyskiwania danych telekomunikacyjnych kontroli sądowej.

Przewodniczący Zespołu poinformował zebranych, iż w odpowiedzi na to wystąpienie Prezes Rady Ministrów nie zgodził się z postulatami subsydiarności, szczególnych uregulowań dotyczących adwokatów i dziennikarzy oraz wskazał na nieefektywność – ze względu na dużą ilość takich spraw – ewentualnej kontroli sądowej. Prezes Rady Ministrów zgodził się natomiast z koniecznością wprowadzenia uregulowań w zakresie niszczenia danych, które nie zostały wykorzystane oraz zbudowania mechanizmów kontroli przestrzegania tego wymogu i ograniczenia zakresu spraw, w których uprawnione instytucje mogłyby pozyskiwać dane telekomunikacyjne. W związku z powyższym Prezes Rady Ministrów polecił dokonanie przeglądu obecnych rozwiązań prawnych w zakresie pozyskiwania danych telekomunikacyjnych i przedstawienie propozycji zmian uwzględniających stanowisko wyrażone w odpowiedzi dla RPO.

Na tej podstawie Przewodniczący Zespołu zwrócił się do jego członków o przedstawienie stanowiska w sprawie zmiany przepisów dotyczących wykorzystywania danych telekomunikacyjnych przez poszczególne instytucje.

Ponadto Przewodniczący Zespołu zwrócił się do Ministerstwa Spraw Zagranicznych i Agencji Wywiadu o dokonanie przeglądu uregulowań prawnych w zakresie pozyskiwania danych telekomunikacyjnych funkcjonujących w innych państwach Unii Europejskiej.

W okresie między pierwszy a drugim posiedzeniem Zespołu uzyskano informacje o rozwiązaniach obowiązujących za granicą. Oprócz materiałów z Agencji Wywiadu i Ministerstwa Spraw Zagranicznych zamówiono dwie pogłębione ekspertyzy dotyczące rozwiązań zagranicznych, w tym wyroków sądów konstytucyjnych w innych krajach: z Ośrodka Studiów Wschodnich dotyczącą krajów, które pozostają w zakresie zainteresowań Ośrodka, oraz od prof. Andrzeja Adamskiego z UMK w Toruniu – znanego eksperta specjalizującego się w problematyce retencji danych telekomunikacyjnych.

Na podstawie uzyskanych danych przeprowadzono analizę rozwiązań zagranicznych. W trzech krajach przepisy dotyczące retencji danych telekomunikacyjnych zostały poddane ocenie sądów konstytucyjnych (w Polsce i na Węgrzech sprawa oczekuje na rozpatrzenie). Spośród tych trzech krajów tylko w Rumunii sąd konstytucyjny uznał retencję jako taką za sprzeczną z zasadami konstytucji, a przede wszystkim z zasadą domniemania niewinności. W Czechach sąd nie ocenił samej retencji, ale całkowicie odrzucił przepisy wdrażające unijną dyrektywę. Natomiast w Niemczech Federalny Trybunał Konstytucyjny nie zakwestionował

retencji, natomiast uchylił szczegółowe przepisy dotyczące retencji z powodu niedostatecznej ochrony gromadzonych danych i zbyt szerokiej możliwości ich wykorzystywania.

Ponieważ 2 kraje nie wdrożyły unijnej dyrektywy, a w 3 wyżej wymienionych sądy konstytucyjne zakwestionowały ustawy ją wdrażające i w żadnym z nich nie wydano jeszcze nowych przepisów, w dalszych analizach można brać pod uwagę 21 krajów. Z tej liczby oprócz Polski tylko w dwóch określono okres retencji na dwa lata (Irlandia, Włochy – ale w obu tych krajach retencja danych internetowych wynosi jeden rok). W 2 krajach retencja odbywa się na okres dłuższy niż rok, w 15 krajach – jeden rok, a w 3 krajach – 6 miesięcy.

Na podstawie zgromadzonych dotychczas danych można stwierdzić, że co najmniej w 11 krajach możliwość dostępu do danych telekomunikacyjnych została ograniczona do przypadków ścigania poważnych przestępstw, na ogół definiowanych poprzez określenie górnej granicy zagrożenia karą pozbawienia wolności (od roku do 5 lat). W 2 krajach nie sprecyzowano poważnych przestępstw, a w 6 (w tym Polsce) nie wprowadzono takich ograniczeń zezwalając na dostęp do danych telekomunikacyjnych w ramach ustawowych zadań służb i organów.

W 9 krajach dostęp do danych telekomunikacyjnych wymaga uprzedniej zgody sądu, a w kolejnych 6 krajach – zgody sędziego lub prokuratora (w niektórych z tych krajów nie jest wymagana zgoda na uzyskanie danych abonentów). Należy jednak pamiętać, że w niektórych spośród tych krajów istnieje instytucja sędziów śledczych, na bieżąco nadzorujących postępowanie. W 7 krajach (w tym w Polsce) nie wprowadzono mechanizmów kontroli zewnętrznej przez organy wymiaru sprawiedliwości, natomiast w niektórych istnieją mechanizmy kontroli administracyjnej lub kontroli następczej.

Równocześnie członkowie Zespołu nadesłali opinie na temat możliwości zmian w obowiązujących w Polsce przepisach dotyczących retencji danych telekomunikacyjnych. Przedstawiciele niektórych byli przeciwni jakimkolwiek zmianom obowiązujących obecnie przepisów, ale w części opinii wyrażano gotowość akceptacji ograniczenia wykorzystania danych telekomunikacyjnych do ścigania poważnych przestępstw oraz powołania pełnomocników odpowiedzialnych za kontrolę wykorzystania tych danych.

W dniu 30 maja 2011 r. odbyło się drugie posiedzenie zespołu, podczas którego Przewodniczący Zespołu przedstawił efekty dotychczasowych prac. Po dyskusji, w trakcie której członkowie Zespołu zgłaszali uwagi i wątpliwości związane ze specyfiką pracy reprezentowanych przez nich instytucji, Przewodniczący Zespołu sformułował następujące wnioski:

- Należy dążyć do ograniczenia okresu obowiązkowej retencji danych telekomunikacyjnych do 12 miesięcy.
- Powinno zostać wprowadzone ograniczenie możliwości pozyskiwania danych telekomunikacyjnych do przypadków ścigania przestępstw, których popełnienie zagrożone jest karą o górnej granicy 3 i więcej lat pozbawienia wolności.
- W instytucjach uprawnionych do pozyskiwania takich danych powinni być powoływani niezależni pełnomocnicy nadzorujący prawidłowość działań w tym zakresie, na wzór powołanego w Centralnym Biurze Antykorupcyjnym pełnomocnika ds. ochrony danych osobowych.
- Należy doprecyzować procedury niszczenia zbędnych danych.
- Nie przewiduje się możliwości szczególnego traktowania niektórych grup zawodowych.

Członkowie Zespołu zostali również poproszeni o nadesłanie stanowisk – popartych szczegółowymi analizami wynikającymi z praktyki wykorzystywania przez służby specjalne oraz inne uprawnione organy informacji telekomunikacyjnych – uzasadniających przydatność obowiązku retencji danych telekomunikacyjnych, a także konieczność dostępu służb specjalnych i policyjnych do tych danych dla ścigania sprawców poważnych przestępstw. Materiały te mogłyby być w przyszłości wykorzystane np. w związku z przewidywaną rozprawą przed Trybunałem Konstytucyjnym.

Na podstawie zgromadzonych informacji i analiz, otrzymanych opinii oraz dyskusji na forum Zespołu zostały sformułowane wnioski, które następnie zawarto w dokumencie noszącym nazwę: *„Raport dotyczący retencji danych telekomunikacyjnych. Propozycja wprowadzenia nowych regulacji ograniczających ingerencję organów państwowych w prywatność obywateli oraz wzmacniających mechanizmy kontroli nad służbami specjalnymi w kontekście prac nad zmianą przepisów dotyczących dostępu do danych telekomunikacyjnych”*. Zawartość „Raportu” wykraczała poza zakres prac Zespołu, ponieważ przedstawiał on również wcześniejsze zmiany prawne mające na celu zwiększenie realnej kontroli nad służbami specjalnymi i ograniczenie ich ingerencji w prywatność obywateli, a w końcowej części zawierał propozycję powołania niezależnego organu kontrolującego pracę operacyjną służb specjalnych. Główna jego część poświęcona była jednak postulowanym kierunkom zmiany przepisów prawa regulujących wykorzystywanie przez uprawnione instytucje danych stanowiących tajemnicę telekomunikacyjną.

W odniesieniu do retencji i wykorzystania danych telekomunikacyjnych „Raport” formułował następujące propozycje:

- utrzymanie ustawowego obowiązku gromadzenia, przetwarzania, przechowywania oraz ochrony informacji objętych tajemnicą telekomunikacyjną;
- określenie zakresu kategorii czynów zabronionych, w toku ścigania których możliwe będzie uzyskanie przedmiotowych danych telekomunikacyjnych. Równocześnie sprecyzowanie, iż chodzi o przestępstwa, w których górna granica zagrożenia karą wynosi co najmniej 3 lata pozbawienia wolności;
- skrócenie do jednego roku – z obecnych dwóch lat – okresu obowiązku przechowywania danych przez operatorów;
- wprowadzenie – w każdym z właściwych rzeczowo organów – instytucji pełnomocnika ds. ochrony danych osobowych i danych telekomunikacyjnych na wzór obecnie funkcjonującego w Centralnym Biurze Antykorupcyjnym pełnomocnika ds. ochrony danych osobowych;
- zwiększenie nadzoru prokuratury nad wykorzystaniem danych telekomunikacyjnych;
- wprowadzenie obowiązku niszczenia danych zbędnych;
- wprowadzenie obowiązku podawania do publicznej wiadomości statystyki uzyskanych danych telekomunikacyjnych.

„Raport” został rozesłany do członków Zespołu. Większość zespołu podeszła do sprawy konstruktywnie, zgłaszając merytoryczne uwagi dotyczące poszczególnych proponowanych rozwiązań. Wnioski i uwagi nadesłane od członków Zespołu na temat „Raportu” dotyczyły m.in.:

- propozycji zwiększenia katalogu czynów zabronionych – m.in. o przestępstwa przeciwko wolności seksualnej i obyczajowości, przestępstwa z zakresu ekstremizmu politycznego oraz niektóre przestępstwa penalizowane przez kodeks

karno skarbowy – w ściganiu których możliwe byłoby skorzystanie z danych telekomunikacyjnych. Podniesiono, iż katalog zbudowany jedynie w oparciu o kryterium górnej granicy zagrożenia karą pozbawienia wolności nie obejmowałyby niektórych przestępstw, w toku ścigania których możliwe jest stosowanie kontroli operacyjnej. Zgłoszono postulat przyznania służbom uprawnienia do korzystania z danych telekomunikacyjnych, także w przypadku przestępstw spoza określonego „Raportem” katalogu, o ile danej okoliczności stanu faktycznego nie da się udowodnić przy użyciu innych środków;

- wnikliwego rozważenia – popartego stosowną analizą prawną – propozycji wyłączenia spod definicji tajemnicy telekomunikacyjnej danych abonentów;
- powoływania pełnomocników ds. kontroli wykorzystywania danych telekomunikacyjnych. Zwrócono uwagę, iż w każdej uprawnionej instytucji istnieją pioniry kontroli i audytu i to w ich właściwości rzeczowej leży proponowany zakres regulacji;
- skrócenia okresu retencji danych do 12 miesięcy – podnoszono, że okres ten może okazać się niewystarczający do ścigania wszystkich rodzajów przestępstw;
- propozycji przygotowania corocznego sprawozdania (uwzględniającego stan ochrony danych telekomunikacyjnych, danych osobowych oraz zakresu ich wykorzystywania), przygotowywanego – przez uprawnione podmioty – niezależne od przedsiębiorców telekomunikacyjnych. Powyższe prowadziłyby do opracowania danych dwutorowo (uprawnione podmioty i przedsiębiorcy telekomunikacyjni), co mogłoby skutkować rozbieżnością tychże sprawozdań;
- zwrócenia uwagi na to, iż prace „Zespołu” powinny być skorelowane z pracami, prowadzonymi w tym zakresie w instytucjach Unii Europejskiej.

„Raport” został również przekazany członkom Kolegium do Spraw Służb Specjalnych, którzy wyrazili następujące opinie:

- Minister Obrony Narodowej nie zgłosił zastrzeżeń do treści „Raportu”.
- Minister Spraw Wewnętrznych i Administracji wyraził poparcie dla proponowanych rozwiązań postulując jedynie pewne rozszerzenie katalogu przestępstw, w przypadku ścigania których możliwe będzie wykorzystanie danych telekomunikacyjnych. Postulował także opracowanie trybu niszczenia zbędnych danych telekomunikacyjnych.
- Minister Finansów postulował pozostawienie możliwości wykorzystania danych telekomunikacyjnych do ścigania niektórych przestępstw karno-skarbowych przynoszących poważne straty dla skarbu państwa.
- Minister Spraw Zagranicznych i Szef Biura Bezpieczeństwa Narodowego wyrazili poparcie dla kierunków zmian zaproponowanych w „Raporcie” w zakresie retencji i wykorzystania danych telekomunikacyjnych, postulowali natomiast rozpoczęcie pogłębionej dyskusji na temat inicjatywy powołania organu kontrolującego pracę operacyjną służb specjalnych.

„Raport” został przekazany Rzecznikowi Praw Obywatelskich, Generalnemu Inspektorowi Ochrony Danych Osobowych, a także przedstawicielom środowisk internautów i obrońców praw człowieka oraz dziennikarzom. Został pozytywnie oceniony przez RPO i GIODO. Wśród organizacji społecznych spotkał się natomiast ze zróżnicowanym przyjęciem. Część tych środowisk uznała „Raport” za krok w dobrym kierunku, ale niewystarczający i postulowała całkowitą rezygnację z retencji. Przedstawiciele innych środowisk uważali

natomiast, że zbyt restrykcyjne ograniczenie dostępu do danych telekomunikacyjnych może powodować niezamierzone skutki niekorzystne dla obywateli.

Podczas trzeciego posiedzenia Zespołu, które odbyło się w dniu 28 lipca 2011 r., omówiono dotychczas otrzymane opinie oraz uwagi dotyczące kierunków zmian w przepisach nakreślonych w „Raporcie”.

Uczestnikom posiedzenia zostało przekazane tłumaczenie materiału otrzymanego z MSWiA, zawierającego stanowisko Francji, Wielkiej Brytanii i Irlandii zaprezentowane uczestnikom warsztatów na temat retencji zorganizowanych przez Komisję Europejską. W materiale tym bardzo cenne było przedstawienie konkretnych przypadków, w których w tych trzech krajach retencja okazała się w praktyce niezbędna do wykrycia sprawców poważnych przestępstw. Ponieważ materiały nadesłane do tej pory przez członków zespołu, zawierające argumenty na rzecz utrzymania retencji, okazały się dość ogólne, członkowie Zespołu zostali poproszeni o przekazanie kolejnych opracowań, w których zawarliby opisy – na poziomie jawnym – konkretnych przypadków, w których retencja okazała się niezbędna dla realizacji ich zadań.

Przewodniczący Zespołu zwrócił się do uczestników posiedzenia o nadesłanie propozycji zmian w przepisach dotyczących funkcjonowania reprezentowanych przez nich instytucji, które – realizując kierunek założony w „Raporcie” – mogą uwzględnić szczegółowe uwarunkowania związane ze specyfiką działania poszczególnych służb i organów.

W dniu 13 września 2011 r. odbyło się posiedzenie Kolegium do Spraw Służb Specjalnych, któremu przewodniczył Prezes Rady Ministrów. Członkowie Kolegium, po zapoznaniu się z informacją przedłożoną przez Sekretarza Kolegium - Przewodniczącego Zespołu, przyjęli zaproponowaną przez Premiera konkluzję akceptującą dotychczasowy kierunek prac Zespołu nad zmianami w obowiązujących przepisach dotyczących pozyskiwania danych telekomunikacyjnych.

Na podstawie zebranych materiałów zostały opracowane propozycje zmian w przepisach, które rozesłano członkom Zespołu i poddano pod dyskusję na jego ostatnim posiedzeniu w dniu 28 września 2011 r.

W wyniku dyskusji dokonano następujących zmian w dyskutowanych propozycjach:

- Na wniosek przedstawiciela Straży Granicznej uzupełniono propozycję przepisu dotyczącego możliwości wykorzystywania danych telekomunikacyjnych do ścigania przestępstw, w stosunku do których SG ma prawo do wnioskowania o kontrolę operacyjną analogicznie, jak zaproponowano to w odniesieniu do Policji.
- Na wniosek przedstawiciela Prokuratora Generalnego wprowadzono propozycję nowego przepisu w kodeksie postępowania karnego dotyczącego odrębnego przechowywania danych telekomunikacyjnych nie mających znaczenia dla toczącego się postępowania, zrezygnowano z propozycji powoływania pełnomocnika do spraw kontroli przetwarzania danych osobowych i telekomunikacyjnych w Sądzie Najwyższym oraz doprecyzowano propozycje przepisów dotyczących zakresu zadań pełnomocników w sądach i prokuraturach.
- Na wniosek przedstawiciela Urzędu Komunikacji Elektronicznej zaproponowano zmianę przepisu dotyczącego gromadzenia danych statystycznych na potrzeby Komisji Europejskiej nakładając obowiązek przekazywania odpowiednich danych

na organy uprawnione do ich pozyskiwania zamiast na operatorów telekomunikacyjnych.

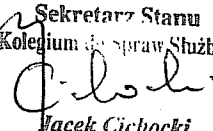
- Na wniosek przedstawiciela Policji dopisano do wszystkich propozycji dotyczących przedstawiania opinii publicznej danych statystycznych dotyczących wykorzystywania danych telekomunikacyjnych delegacji do wydania rozporządzeń określających sposób obliczania tych danych.

Podczas posiedzenia zgłoszono również uwagi i zastrzeżenia, które nie zostały uwzględnione w opracowanych propozycjach zmian przepisów:

- Przedstawiciele Żandarmerii Wojskowej, Ministerstwa Finansów (Wywiadu Skarbowego) oraz Centralnego Biura Antykorupcyjnego postulowali w odniesieniu do swoich służb rozszerzenie możliwości uzyskiwania danych telekomunikacyjnych na przypadki ścigania wszystkich naruszeń prawa, w odniesieniu do których mogą ubiegać się o zgodę na zastosowanie kontroli operacyjnej (propozycja nie została uwzględniona, ponieważ w przypadku tych służb – w odróżnieniu od Policji i Straży Granicznej – przepisy odpowiednich ustaw nie ograniczają się do wskazania konkretnych artykułów kodeksu karnego).
- Przedstawiciel Ministerstwa Finansów wskazywał na duże szkody dla efektywności wykonywania ustawowych zadań przez Wywiad Skarbowy i Służbę Celną w przypadku wejścia w życie proponowanych zmian przepisów, ponieważ większość przypadków wykorzystywania danych telekomunikacyjnych przez te służby wiąże się ze ściganiem przestępstw przynoszących duże straty skarbowi państwa, ale zagrożonych karą niższą niż trzy lata pozbawienia wolności.
- Przedstawiciele Prokuratora Generalnego i Ministerstwa Sprawiedliwości zgłaszali zastrzeżenia dotyczące inicjatywy powołania pełnomocników do spraw kontroli przetwarzania danych osobowych i telekomunikacyjnych w sądach i prokuraturach w kontekście możliwej sprzeczności z zasadą kontroli instancyjnej i postulowali rozważenie ograniczenia roli tych pełnomocników do zbierania danych statystycznych.
- Przedstawiciel Agencji Wywiadu zgłosił ponownie propozycję uregulowania możliwości pozyskiwania danych telekomunikacyjnych przez Agencję Wywiadu.
- Przedstawiciel Agencji Bezpieczeństwa Wewnętrznego zaproponował rozszerzenie możliwości wykorzystywania danych telekomunikacyjnych do ścigania wszystkich przestępstw zagrożonych karą niższą niż trzy lata pozbawienia wolności, jeżeli ustalenie okoliczności faktycznych za pomocą innych dowodów byłoby niemożliwe albo szczególnie utrudnione.

Propozycje zmian w obowiązujących przepisach w wersji zawierającej poprawki uwzględnione w wyniku dyskusji podczas ostatniego posiedzenia Zespołu zostaną przedłożone Prezesowi Rady Ministrów, a następnie rozesłane członkom Zespołu oraz kierownikom delegujących ich instytucji, Rzecznikowi Praw Obywatelskich i Generalnemu Inspektorowi Ochrony Danych Osobowych. Będą one mogły w nadchodzącej kadencji Sejmu stać się podstawą do opracowania projektów założeń nowelizacji Prawa telekomunikacyjnego, Kodeksu postępowania karnego oraz ustaw regulujących działanie służb i organów uprawnionych do pozyskiwania danych telekomunikacyjnych.

W załączeniu: propozycje zmian w obowiązujących przepisach.

Sekretarz Stanu
Sekretarz Kolegium ds. Spraw Służb Specjalnych

Jacek Cichoński

**Propozycje zmiany przepisów ustaw regulujących dostęp do danych
zachowywanych przez podmioty wykonujące działalność telekomunikacyjną**

**Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz
Agencji Wywiadu (Dz. U. z 2010 nr 29, poz. 154, j.t. z późn. zm.)**

W art. 28 nadaje się nowe brzmienie ust. 1:

Obowiązek uzyskania zgody sądu, o której mowa w art. 27 ust. 1, nie dotyczy informacji niezbędnych do realizacji przez ABW zadań:

- 1) rozpoznawania, zapobiegania i zwalczania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa i jego porządek konstytucyjny, wynikających ze szpiegostwa lub terroryzmu, a także rozpoznawania, zapobiegania i wykrywania przestępstw, o których mowa w art. 5 ust. 1 pkt 2 zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata oraz przestępstw popełnianych za pomocą środków komunikacji elektronicznej, w postaci danych o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.) zwanych dalej „danymi telekomunikacyjnymi”, z zastrzeżeniem pkt 2;
- 2) o których mowa w art. 5 ust. 1, w postaci danych:
 - a) telekomunikacyjnych dotyczących użytkownika,
 - b) identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.

W art. 28 po ust. 4 dodaje się nowy ust. 5:

Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które zawierają dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego ABW przekazuje prokuratorowi oraz informuje go o wszystkich przypadkach wystąpienia o dane telekomunikacyjne w sprawie, w której uzyskano dane telekomunikacyjne podlegające przekazaniu.

Po art. 34 dodaje się nowe art. 34a i 34b:

34a:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania danych osobowych i telekomunikacyjnych przez ABW albo AW z przepisami ustaw sprawuje pełnomocnik do spraw kontroli przetwarzania danych osobowych i telekomunikacyjnych, powoływany odrębnie dla ABW i AW, zwany dalej "pełnomocnikiem".
2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Szefowie Agencji powołują pełnomocników spośród podległych im funkcjonariuszy. Zwolnienie ze służby, z wyłączeniem przypadków, o których mowa w art. 60 ust. 1 pkt 1, 4 i

- 5 lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Prezesa Rady Ministrów.
4. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez ABW albo AW danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
 5. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez ABW albo AW.
 6. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Prezesa Rady Ministrów i Szefa ABW albo AW, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.
 7. Pełnomocnik ma prawo w szczególności do:
 - 1) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - 2) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych ABW albo AW;
 - 3) żądania pisemnych wyjaśnień.
 8. Pełnomocnik przedstawia corocznie do dnia 31 marca Prezesowi Rady Ministrów, Sejmowej Komisji do Spraw Służb Specjalnych, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Szefa ABW albo AW sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w ABW albo AW oraz wszystkie przypadki naruszenia przepisów w tym zakresie.
 9. Pełnomocnik powołany w ABW przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem Szefa ABW dane statystyczne dotyczące liczby osób, w stosunku do których ABW w poprzednim roku uzyskiwała dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
 10. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.
 11. Pełnomocnik powołany w ABW przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Szefa ABW dane statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

34b:

1. Agencje przetwarzają dane osobowe i dane telekomunikacyjne przez okres, w którym są one niezbędne do realizacji ich ustawowych zadań. Agencje dokonują, nie rzadziej niż co 5 lat, weryfikacji potrzeby dalszego przetwarzania tych danych, usuwając dane zbędne.
2. Po dokonaniu weryfikacji dane zbędne usuwają niezwłocznie komisje powołane przez Szefów Agencji. Z czynności komisji sporządza się protokół zawierający w szczególności wykaz zniszczonych dokumentów lub nośników informatycznych zawierających te dane oraz sposób ich zniszczenia.
3. Przetwarzane przez ABW dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową oraz dane o stanie zdrowia, nałogach lub życiu seksualnym osób podejrzanych o popełnienie przestępstw, które nie zostały skazane za te przestępstwa, a także

dane telekomunikacyjne, podlegają komisijnemu i protokolarnemu zniszczeniu niezwłocznie po uprawnieniu się stosownego orzeczenia.

Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2006 r. nr 104, poz. 709, z późn. zm.)

W art. 32 nadaje się nowe brzmienie ust. 1:

Obowiązek uzyskania zgody sądu, o której mowa w art. 31 ust. 1, nie dotyczy informacji niezbędnych do realizacji przez SKW zadań:

- 1) rozpoznawania, zapobiegania oraz wykrywania popełnianych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników SZ RP i innych jednostek organizacyjnych MON, przestępstw szpiegostwa lub terroryzmu, a także rozpoznawania, zapobiegania i wykrywania innych przestępstw, o których mowa w art. 5 ust. 1 pkt 1 zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata lub popełnianych za pomocą środków komunikacji elektronicznej, w postaci danych o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.) zwanych dalej „danymi telekomunikacyjnymi”, z zastrzeżeniem pkt 2;
- 2) o których mowa w art. 5 ust. 1, w postaci danych:
 - a) telekomunikacyjnych dotyczących użytkownika,
 - b) identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.

W art. 32 po ust. 6 dodaje się nowy ust. 7:

Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które zawierają dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego SKW przekazuje prokuratorowi oraz informuje go o wszystkich przypadkach wystąpienia o dane telekomunikacyjne w sprawie, w której uzyskano dane telekomunikacyjne podlegające przekazaniu.

Po art. 38 dodaje się nowe art. 38a i 38b:

art. 38a:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania danych osobowych i telekomunikacyjnych przez SKW albo SWW z przepisami ustaw sprawuje pełnomocnik do spraw kontroli przetwarzania danych osobowych i telekomunikacyjnych, powoływany odrębnie dla SKW i SWW, zwany dalej "pełnomocnikiem".
2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Szefowie Służb powołują pełnomocników spośród podległych im funkcjonariuszy. Zwolnienie ze służby lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Ministra Obrony Narodowej.

4. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez SKW albo SWW danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
5. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez SKW albo SWW.
6. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Ministra Obrony Narodowej i Szefa SKW albo SWW, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.
7. Pełnomocnik ma prawo w szczególności do:
 - 1) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - 2) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych SKW albo SWW;
 - 3) żądania pisemnych wyjaśnień.
8. Pełnomocnik przedstawia corocznie do dnia 31 marca Ministrowi Obrony Narodowej, Sejmowej Komisji do Spraw Służb Specjalnych, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Szefa SKW albo SWW sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w SKW albo SWW oraz wszystkie przypadki naruszenia przepisów w tym zakresie.
9. Pełnomocnik powołany w SKW przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem Szefa SKW dane statystyczne dotyczące liczby osób, w stosunku do których SKW w poprzednim roku uzyskiwała dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
10. Minister Obrony Narodowej określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.
11. Pełnomocnik powołany w SKW przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Szefa SKW dane statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

art. 38b:

1. Służby przetwarzają dane osobowe i dane telekomunikacyjne przez okres, w którym są one niezbędne do realizacji ich ustawowych zadań. Służby dokonują, nie rzadziej niż co 5 lat, weryfikacji potrzeby dalszego przetwarzania tych danych, usuwając dane zbędne.
2. Po dokonaniu weryfikacji dane zbędne usuwają niezwłocznie komisje powołane przez Szefów Służb. Z czynności komisji sporządza się protokół zawierający w szczególności wykaz zniszczonych dokumentów lub nośników informatycznych zawierających te dane oraz sposób ich zniszczenia.
3. Przetwarzane przez SKW dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową oraz dane o stanie zdrowia, nałogach lub życiu seksualnym osób podejrzanych o popełnienie przestępstw, które nie zostały skazane za te przestępstwa, a także dane telekomunikacyjne, podlegają komisijnemu i protokolarnemu zniszczeniu niezwłocznie po uprawomocnieniu się stosownego orzeczenia.

Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2006 r. nr 104, poz. 708, z późn. zm.)

W art. 18 nadaje się nowe brzmienie ust. 1:

Obowiązek uzyskania zgody sądu, o której mowa w art. 17, nie dotyczy informacji niezbędnych do realizacji przez CBA zadań:

- 1) rozpoznawania, zapobiegania i wykrywania przestępstw, o których mowa w art. 2 ust. 1 zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata oraz przestępstw popełnianych za pomocą środków komunikacji elektronicznej, w postaci danych o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.) zwanych dalej „danymi telekomunikacyjnymi”, z zastrzeżeniem pkt 2;
- 2) o których mowa w art. 2 ust. 1, w postaci danych:
 - a) telekomunikacyjnych dotyczących użytkownika,
 - b) identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.

W art. 18 po ust. 4 dodaje się nowy ust. 5:

Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które zawierają dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego CBA przekazuje prokuratorowi oraz informuje go o wszystkich przypadkach wystąpienia o dane telekomunikacyjne w sprawie, w której uzyskano dane telekomunikacyjne podlegające przekazaniu.

Nadaje się nowe brzmienie art. 22b:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania danych osobowych i telekomunikacyjnych przez CBA z przepisami ustaw sprawuje pełnomocnik do spraw kontroli przetwarzania przez CBA danych osobowych i telekomunikacyjnych, zwany dalej "pełnomocnikiem".
2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Szef CBA powołuje pełnomocnika spośród funkcjonariuszy CBA. Zwolnienie ze służby, z wyłączeniem przypadków, o których mowa w art. 64 ust. 1 pkt 1, 4, 5 i 6, lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Prezesa Rady Ministrów po zasięgnięciu opinii Sejmowej Komisji do Spraw Służb Specjalnych.
4. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez CBA danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
5. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez CBA.
6. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Prezesa Rady Ministrów i Szefa CBA, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.

7. Pełnomocnik ma prawo w szczególności do:
 - 1) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - 2) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych CBA;
 - 3) żądania pisemnych wyjaśnień.
8. Pełnomocnik przedstawia corocznie do dnia 31 marca Prezesowi Rady Ministrów, Sejmowej Komisji do Spraw Służb Specjalnych, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Szefa CBA sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w CBA oraz wszystkie przypadki naruszenia przepisów w tym zakresie.
9. Pełnomocnik przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem Szefa CBA dane statystyczne dotyczące liczby osób, w stosunku do których CBA w poprzednim roku uzyskiwała dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
10. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.
11. Pełnomocnik przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Szefa CBA dane statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U z 2007 nr 43, poz. 277, j.t. z późn. zm.)

W art. 20c nadaje się nowe brzmienie ust. 1:

W celu zapobiegania lub wykrywania przestępstw zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej "danymi telekomunikacyjnymi", oraz może je przetwarzać.

W art. 20c po ust. 1 dodaje się nowy ust. 1a:

Ograniczenie wynikające z ust. 1 nie dotyczy przypadków zagrożenia zdrowia lub życia, udostępniania danych telekomunikacyjnych dotyczących użytkownika oraz zapobiegania i wykrywania przestępstw, o których mowa w art. 19 ust. 1 lub przestępstw popełnianych za pomocą środków komunikacji elektronicznej.

W art. 20c nadaje się nowe brzmienie ust. 6:

Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które zawierają dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego Komendant Główny Policji lub komendant wojewódzki Policji przekazuje prokuratorowi właściwemu miejscowo i rzeczowo oraz informuje prokuratora o wszystkich

przypadkach wystąpienia o dane telekomunikacyjne w sprawie, w której uzyskano dane telekomunikacyjne podlegające przekazaniu.

Po art. 20c dodaje się nowy art. 20ca:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania danych osobowych i telekomunikacyjnych przez Policję z przepisami ustaw sprawuje pełnomocnik do spraw kontroli przetwarzania przez Policję danych osobowych i telekomunikacyjnych, zwany dalej "pełnomocnikiem".
2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Komendant Główny Policji powołuje pełnomocnika spośród funkcjonariuszy Policji. Zwolnienie ze służby, z wyłączeniem przypadków, o których mowa w art. 41 ust. 1 pkt 1, 4, 4a i 5, lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Ministra Spraw Wewnętrznych i Administracji.
4. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez Policję danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
5. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez Policję.
6. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Ministra Spraw Wewnętrznych i Administracji i Komendanta Głównego Policji, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.
7. Pełnomocnik ma prawo w szczególności do:
 - 1) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - 2) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych Policji;
 - 3) żądania pisemnych wyjaśnień.
8. Pełnomocnik przedstawia corocznie do dnia 31 marca Ministrowi Spraw Wewnętrznych i Administracji, Sejmowej Komisji Administracji i Spraw Wewnętrznych, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Komendanta Głównego Policji sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w Policji oraz wszystkie przypadki naruszenia przepisów w tym zakresie.
9. Pełnomocnik przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem Komendanta Głównego Policji dane statystyczne dotyczące liczby osób, w stosunku do których Policja w poprzednim roku uzyskiwała dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
10. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.

11. Pełnomocnik przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Komendanta Głównego Policji dane statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 nr 116, poz. 675, j.t. z późn. zm.)

W art. 10b nadaje się nowe brzmienie ust. 1:

W celu zapobiegania lub wykrywania przestępstw zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata Straż Graniczna może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej "danymi telekomunikacyjnymi", oraz może je przetwarzać.

W art. 10b po ust. 1 dodaje się nowe ust. 1a i 1b:

1a:

Ograniczenie wynikające z ust. 1 nie dotyczy przypadków zagrożenia zdrowia lub życia, udostępniania danych telekomunikacyjnych dotyczących użytkownika oraz zapobiegania i wykrywania przestępstw, o których mowa w art. 9e ust. 1 lub popełnianych za pomocą środków komunikacji elektronicznej.

1b:

Podmiot prowadzący działalność telekomunikacyjną udostępnia nieodpłatnie dane telekomunikacyjne:

- 1) funkcjonariuszowi wskazanemu w pisemnym wniosku Komendanta Głównego Straży Granicznej lub komendanta oddziału Straży Granicznej albo osoby przez nich upoważnionej,
- 2) na ustne żądanie funkcjonariusza posiadającego pisemne upoważnienie osób, o których mowa w pkt 1,
- 3) za pośrednictwem sieci telekomunikacyjnej funkcjonariuszowi posiadającemu pisemne upoważnienie osób, o których mowa w pkt 1.

W art. 10b nadaje się nowe brzmienie ust. 5:

Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 1b, które zawierają dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego Komendant Główny Straży Granicznej lub komendant oddziału Straży Granicznej przekazuje prokuratorowi właściwemu ze względu na siedzibę organu przekazującego oraz informuje prokuratora o wszystkich przypadkach wystąpienia o dane telekomunikacyjne w sprawie, w której uzyskano dane telekomunikacyjne podlegające przekazaniu.

Po art. 10b dodaje się nowy art. 10ba:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania danych osobowych i telekomunikacyjnych przez Straż Graniczną z przepisami ustaw sprawuje pełnomocnik do

- spraw kontroli przetwarzania przez Straż Graniczną danych osobowych i telekomunikacyjnych, zwany dalej "pełnomocnikiem".
2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
 3. Komendant Główny Straży Granicznej powołuje pełnomocnika spośród funkcjonariuszy Straży Granicznej. Zwolnienie ze służby, z wyłączeniem przypadków, o których mowa w art. 45 ust. 1 pkt 1, 4, i 5, lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Ministra Spraw Wewnętrznych i Administracji.
 4. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez Straż Graniczną danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
 5. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez Straż Graniczną.
 6. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Ministra Spraw Wewnętrznych i Administracji i Komendanta Głównego Straży Granicznej, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.
 7. Pełnomocnik ma prawo w szczególności do:
 - 1) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - 2) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych Straży Granicznej;
 - 3) żądania pisemnych wyjaśnień.
 8. Pełnomocnik przedstawia corocznie do dnia 31 marca Ministrowi Spraw Wewnętrznych i Administracji, Sejmowej Komisji Administracji i Spraw Wewnętrznych, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Komendanta Głównego Straży Granicznej sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w Policji oraz wszystkie przypadki naruszenia przepisów w tym zakresie.
 9. Pełnomocnik przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem Komendanta Głównego Straży Granicznej dane statystyczne dotyczące liczby osób, w stosunku do których Straż Graniczna w poprzednim roku uzyskiwała dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
 10. Minister właściwy do spraw wewnętrznych określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.
 11. Pełnomocnik przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Komendanta Głównego Straży Granicznej dane statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych. (Dz. U. z 2001 r. nr 123, poz. 1353, z późn. zm.)

W art. 30 nadaje się nowe brzmienie ust. 1:

W celu zapobiegania lub wykrywania przestępstw zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata Żandarmeria Wojskowa może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej "danymi telekomunikacyjnymi", oraz może je przetwarzać.

W art. 30 po ust. 1 dodaje się nowy ust. 1a:

Ograniczenie wynikające z ust. 1 nie dotyczy przypadków zagrożenia zdrowia lub życia, udostępniania danych telekomunikacyjnych dotyczących użytkownika oraz zapobiegania i wykrywania przestępstw popełnianych za pomocą środków komunikacji elektronicznej.

W art. 30 nadaje się nowe brzmienie ust. 5:

Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które zawierają dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego Żandarmeria Wojskowa przekazuje właściwemu prokuratorowi wojskowemu oraz informuje go o wszystkich przypadkach wystąpienia o dane telekomunikacyjne w sprawie, w której uzyskano dane telekomunikacyjne podlegające przekazaniu.

Po art. 30a dodaje się nowy art. 30aa:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania danych osobowych i telekomunikacyjnych przez Żandarmerię Wojskową z przepisami ustaw sprawuje pełnomocnik do spraw kontroli przetwarzania przez Żandarmerię Wojskową danych osobowych i telekomunikacyjnych, zwany dalej "pełnomocnikiem".
2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Komendant Główny Żandarmerii Wojskowej powołuje pełnomocnika spośród podległych mu żołnierzy ŻW. Zwolnienie ze służby lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Ministra Obrony Narodowej.
4. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez Żandarmerię Wojskową danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
5. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez Żandarmerię Wojskową.
6. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Ministra Obrony Narodowej i Komendanta Głównego Żandarmerii Wojskowej, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.

7. Pełnomocnik ma prawo w szczególności do:
 - 1) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - 2) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych Żandarmerii Wojskowej;
 - 3) żądania pisemnych wyjaśnień.
8. Pełnomocnik przedstawia corocznie do dnia 31 marca Ministrowi Obrony Narodowej, Sejmowej Komisji Obrony Narodowej, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Komendanta Głównego Żandarmerii Wojskowej sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w Żandarmerii Wojskowej oraz wszystkie przypadki naruszenia przepisów w tym zakresie.
9. Pełnomocnik przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem Komendanta Głównego Żandarmerii Wojskowej dane statystyczne dotyczące liczby osób, w stosunku do których Żandarmeria Wojskowa w poprzednim roku uzyskiwała dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
10. Minister Obrony Narodowej określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.
11. Pełnomocnik przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Komendanta Głównego Żandarmerii Wojskowej dane statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

Ustawa z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 nr 41, poz. 214 j.t.)

W art. 36b nadaje się nowe brzmienie ust. 1:

W celu zapobiegania lub wykrywania przestępstw i przestępstw skarbowych, których zwalczanie należy do właściwości wywiadu skarbowego, zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata, wywiad skarbowy może mieć udostępniane dane:

- 1) o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej "danymi telekomunikacyjnymi",
 - 2) identyfikujące podmiot korzystający z usług pocztowych oraz dotyczące faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług
- oraz może je przetwarzać.

W art. 36b po ust. 1 dodaje się nowy ust. 1a:

Ograniczenie wynikające z ust. 1 nie dotyczy udostępniania danych telekomunikacyjnych dotyczących użytkownika oraz zapobiegania i wykrywania przestępstw popełnianych za pomocą środków komunikacji elektronicznej.

Po art. 36b dodaje się nowe art. 36ba i 36bb:

art. 36ba:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania danych osobowych i telekomunikacyjnych przez wywiad skarbowy z przepisami ustaw sprawuje pełnomocnik do spraw kontroli przetwarzania przez wywiad skarbowy danych osobowych i telekomunikacyjnych, zwany dalej "pełnomocnikiem".
2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Generalny Inspektor Kontroli Skarbowej powołuje pełnomocnika spośród pracowników wywiadu skarbowego. Zwolnienie lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Ministra właściwego do spraw finansów publicznych.
4. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez wywiad skarbowy danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
5. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez wywiad skarbowy.
6. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Ministra właściwego do spraw finansów publicznych i Generalnego Inspektora Kontroli Skarbowej, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.
7. Pełnomocnik ma prawo w szczególności do:
 - 1) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - 2) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych wywiadu skarbowego;
 - 3) żądania pisemnych wyjaśnień.
8. Pełnomocnik przedstawia corocznie do dnia 31 marca Ministrowi właściwemu do spraw finansów publicznych, Sejmowej Komisji Finansów Publicznych, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Generalnego Inspektora Kontroli Skarbowej sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w wywiadzie skarbowym oraz wszystkie przypadki naruszenia przepisów w tym zakresie.
9. Pełnomocnik przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem Generalnego Inspektora Kontroli Skarbowej dane statystyczne dotyczące liczby osób, w stosunku do których wywiad skarbowy w poprzednim roku uzyskiwał dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
10. Minister właściwy do spraw finansów publicznych określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.
11. Pełnomocnik przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Generalnego Inspektora Kontroli Skarbowej dane

statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

art. 36bb:

1. Wywiad skarbowy przetwarza dane osobowe i dane telekomunikacyjne przez okres, w którym są one niezbędne do realizacji jego ustawowych zadań. Wywiad skarbowy dokonuje, nie rzadziej niż co 5 lat, weryfikacji potrzeby dalszego przetwarzania tych danych, usuwając dane zbędne.
2. Po dokonaniu weryfikacji dane zbędne usuwają niezwłocznie komisje powołane przez Generalnego Inspektora Kontroli Skarbowej. Z czynności komisji sporządza się protokół zawierający w szczególności wykaz zniszczonych dokumentów lub nośników informatycznych zawierających te dane oraz sposób ich zniszczenia.

W art. 36b po ust. 2 dodaje się nowy ust. 2a:

Materiały uzyskane w wyniku czynności podjętych na podstawie art. 36b ust. 2, które zawierają dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego wywiad skarbowy przekazuje prokuratorowi oraz informuje go o wszystkich przypadkach wystąpienia o dane telekomunikacyjne w sprawie, w której uzyskano dane telekomunikacyjne podlegające przekazaniu.

Ustawa z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2009 r. nr 168, poz. 1323, z późn. zm.)

W art. 75d nadaje się nowe brzmienie ust. 1:

W celu zapobiegania lub wykrywania przestępstw i przestępstw skarbowych, których zwalczanie należy do właściwości Służby Celnej, zagrożonych karą pozbawienia wolności, której górna granica wynosi co najmniej 3 lata, Służba Celna może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), zwane dalej "danymi telekomunikacyjnymi", oraz może je przetwarzać.

W art. 75d po ust. 1 dodaje się nowy ust. 1a:

Ograniczenie wynikające z ust. 1 nie dotyczy udostępniania danych telekomunikacyjnych dotyczących użytkownika oraz zapobiegania i wykrywania przestępstw popełnianych za pomocą środków komunikacji elektronicznej.

W art. 75d po ust. 4 dodaje się nowy ust. 4a:

Materiały uzyskane w wyniku czynności podjętych na podstawie ust. 2, które zawierają dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania karnego Służba Celna przekazuje prokuratorowi oraz informuje go o wszystkich przypadkach wystąpienia o dane telekomunikacyjne w sprawie, w której uzyskano dane telekomunikacyjne podlegające przekazaniu.

Po art. 75d dodaje się nowy art. 75da:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania danych osobowych i telekomunikacyjnych przez Służbę Celną z przepisami ustaw sprawuje pełnomocnik do spraw kontroli przetwarzania przez Służbę Celną danych osobowych i telekomunikacyjnych, zwany dalej "pełnomocnikiem".
2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Szef Służby Celnej powołuje pełnomocnika spośród funkcjonariuszy Służby Celnej. Zwolnienie lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Ministra właściwego do spraw finansów publicznych.
4. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez Służbę Celną danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
5. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez Służbę Celną.
6. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Ministra właściwego do spraw finansów publicznych i Szefa Służby Celnej, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.
7. Pełnomocnik ma prawo w szczególności do:
 - 1) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - 2) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych Służby Celnej;
 - 3) żądania pisemnych wyjaśnień.
8. Pełnomocnik przedstawia corocznie do dnia 31 marca Ministrowi właściwemu do spraw finansów publicznych, Sejmowej Komisji Finansów Publicznych, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Szefa Służby Celnej sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w Służbie Celnej oraz wszystkie przypadki naruszenia przepisów w tym zakresie.
9. Pełnomocnik przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem Szefa Służby Celnej dane statystyczne dotyczące liczby osób, w stosunku do których Służba Celną w poprzednim roku uzyskiwała dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
10. Minister właściwy do spraw finansów publicznych określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.
11. Pełnomocnik przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem Szefa Służby Celnej dane statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. nr 89, poz. 555, z późn. zm.)

W art. 218 nadaje się nowe brzmienie § 1:

Przedsiębiorcy telekomunikacyjni obowiązani są udostępnić sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.) zwane dalej „danymi telekomunikacyjnymi”, jeżeli mają znaczenie dla toczącego się postępowania w sprawie przestępstwa zagrożonego karą pozbawiania wolności, której górna granica wynosi co najmniej 3 lata, przestępstw popełnianych za pomocą środków komunikacji elektronicznej lub gdy ustalenie określonej okoliczności faktycznej innymi dowodami jest niemożliwe lub szczególnie utrudnione.

W art. 218 po § 1 dodaje się nowy § 1a:

Urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celne oraz instytucje i przedsiębiorstwa transportowe obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, korespondencję i przesyłki oraz dane telekomunikacyjne dotyczące użytkownika, jeżeli mają znaczenie dla toczącego się postępowania. Tylko sąd lub prokurator mają prawo je otwierać lub zarządzić ich otwarcie.

W art. 218 po § 3 dodaje się nowy § 4:

Dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.), które nie mają znaczenia dla toczącego się postępowania, wyłącza się z jego akt i przechowuje odrębnie, przy czym dostęp do nich mogą mieć tylko strony postępowania. Okres przechowywania tych danych jest tożsamy z okresem przechowywania akt postępowania, po czym ulegają one komisyjnemu zniszczeniu.

Ustawa z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz. U. z 2001 r. nr 98, poz. 1080, z późn. zm.)

Po art. 20 dodaje się nowy art. 20a:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania przez sądy danych osobowych oraz danych, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2004 r. nr 171, poz. 1800, z późn. zm.) zwanych dalej „danymi telekomunikacyjnymi”, z przepisami ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 1997 r. nr 101, poz. 926, z późn. zm.), ustawy – Prawo telekomunikacyjne oraz z art. 218 §4 kodeksu postępowania karnego, sprawuje pełnomocnik do spraw kontroli przetwarzania przez sądy danych osobowych i telekomunikacyjnych, zwany dalej „pełnomocnikiem”.
2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

3. Prezes sądu apelacyjnego powołuje pełnomocnika właściwego dla sądów powszechnych obszaru apelacji spośród sędziów sądu apelacyjnego. Zwolnienie lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Ministra Sprawiedliwości.
4. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez sądy danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
5. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez sądy, dla których jest właściwy.
6. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Ministra Sprawiedliwości, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.
7. Pełnomocnik ma prawo w szczególności do:
 - a) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - b) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych sądów;
 - c) żądania pisemnych wyjaśnień.
8. Pełnomocnik przedstawia corocznie do dnia 31 marca Ministrowi Sprawiedliwości, Sejmowej Komisji Sprawiedliwości i Praw Człowieka, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem prezesa sądu sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w sądach oraz wszystkie przypadki naruszenia przepisów w tym zakresie.
9. Pełnomocnik przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem prezesa sądu dane statystyczne dotyczące liczby osób, w stosunku do których sądy w poprzednim roku uzyskiwały dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
10. Minister Sprawiedliwości określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.
11. Pełnomocnik przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem prezesa sądu dane statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

Ustawa z dnia 21 sierpnia 1997 r. Prawo o ustroju sądów wojskowych (Dz. U. z 2007 r. nr 226, poz. 1676, j.t. z późn zm.)

Po art. 18 dodaje się nowy art. 18a:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania przez sądy wojskowe danych osobowych oraz danych, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.) zwanych dalej „danymi telekomunikacyjnymi”, z przepisami ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 1997 r. nr 101, poz. 926, z późn. zm.), ustawy – Prawo telekomunikacyjne

oraz z art. 218 §4 kodeksu postępowania karnego, sprawuje pełnomocnik do spraw kontroli przetwarzania przez sądy wojskowe danych osobowych i telekomunikacyjnych, zwany dalej "pełnomocnikiem".

2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Prezes wojskowego sądu okręgowego powołuje pełnomocnika właściwego dla sądów danego okręgu spośród sędziów wojskowego sądu okręgowego. Zwolnienie lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Ministra Sprawiedliwości.
4. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez sądy wojskowe danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
5. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez sądy wojskowe, dla których jest właściwy.
6. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Ministra Sprawiedliwości, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.
7. Pełnomocnik ma prawo w szczególności do:
 - 1) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - 2) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych sądów wojskowych;
 - 3) żądania pisemnych wyjaśnień.
8. Pełnomocnik przedstawia corocznie do dnia 31 marca Ministrowi Sprawiedliwości, Sejmowej Komisji Sprawiedliwości i Praw Człowieka, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem prezesa wojskowego sądu okręgowego sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w sądach wojskowych oraz wszystkie przypadki naruszenia przepisów w tym zakresie.
9. Pełnomocnik przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem prezesa wojskowego sądu okręgowego dane statystyczne dotyczące liczby osób, w stosunku do których sądy w poprzednim roku uzyskiwały dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
10. Minister Sprawiedliwości określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.
11. Pełnomocnik przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem prezesa wojskowego sądu okręgowego dane statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

Ustawa z dnia 20 czerwca 1985 r. o prokuraturze (Dz. U. z 2008 r. nr 7, poz. 39, j.t. z późn. zm.)

Po art. 18 dodaje się nowy art. 18a:

1. Nadzór nad zgodnością pozyskiwania oraz przetwarzania przez prokuraturę danych osobowych oraz danych, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.) zwanych dalej „danymi telekomunikacyjnymi”, z przepisami ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. z 1997 r. nr 101, poz. 926, z późn. zm.), ustawy – Prawo telekomunikacyjne oraz z art. 218 §4 kodeksu postępowania karnego, sprawuje pełnomocnik do spraw kontroli przetwarzania przez prokuraturę danych osobowych i telekomunikacyjnych, zwany dalej "pełnomocnikiem".
2. Pełnomocnik wykonuje również obowiązki i przysługują mu uprawnienia administratora bezpieczeństwa informacji, o którym mowa w art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.
3. Prokurator apelacyjny powołuje pełnomocnika właściwego dla prokuratur danego okręgu apelacji spośród prokuratorów prokuratury apelacyjnej. Zwolnienie lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Prokuratora Generalnego.
4. Naczelny Prokurator Wojskowy powołuje pełnomocnika właściwego dla prokuratury wojskowej spośród prokuratorów prokuratury wojskowej. Zwolnienie lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Prokuratora Generalnego.
5. Prokurator Generalny powołuje pełnomocnika właściwego dla Prokuratury Generalnej spośród prokuratorów Prokuratury Generalnej. Zwolnienie lub odwołanie pełnomocnika z pełnionej funkcji następuje za zgodą Prezydenta Rzeczypospolitej Polskiej.
6. W ramach nadzoru pełnomocnik prowadzi rzetelną, obiektywną i niezależną kontrolę prawidłowości pozyskiwania i przetwarzania przez prokuraturę danych osobowych i telekomunikacyjnych, a w szczególności ich przechowywania, weryfikacji i usuwania.
7. Pełnomocnik otrzymuje informacje o wszystkich przypadkach pozyskiwania danych telekomunikacyjnych przez prokuratury dla których jest właściwy.
8. W przypadku stwierdzenia naruszenia przepisów ustawy oraz przepisów o ochronie danych osobowych lub danych stanowiących tajemnicę telekomunikacyjną pełnomocnik podejmuje działania zmierzające do wyjaśnienia okoliczności tego naruszenia, zawiadamiając o tym niezwłocznie Prokuratora Generalnego, a w razie uzasadnionego podejrzenia popełnienia przestępstwa, właściwą jednostkę organizacyjną prokuratury.
9. Pełnomocnik ma prawo w szczególności do:
 - 1) wglądu do wszelkich dokumentów związanych z wykonywaną kontrolą;
 - 2) swobodnego wstępu do pomieszczeń i obiektów kontrolowanych komórek organizacyjnych prokuratury;
 - 3) żądania pisemnych wyjaśnień.
10. Pełnomocnik przedstawia corocznie do dnia 31 marca Prokuratorowi Generalnemu, Sejmowej Komisji Sprawiedliwości i Praw Człowieka, Generalnemu Inspektorowi Ochrony Danych Osobowych oraz Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem prokuratora który go powołał sprawozdanie za poprzedni rok kalendarzowy, w którym omawia stan ochrony danych osobowych i telekomunikacyjnych w prokuraturze oraz wszystkie przypadki naruszenia przepisów w tym zakresie.

11. Pełnomocnik przekazuje corocznie do dnia 31 marca do wiadomości publicznej za pośrednictwem prokuratora który go powołał dane statystyczne dotyczące liczby osób, w stosunku do których prokuratura w poprzednim roku uzyskiwała dane telekomunikacyjne z wyłączeniem danych dotyczących użytkownika, w tym liczby osób, w stosunku do których uzyskano dane dotyczące lokalizacji oraz dane o połączeniach.
12. Minister Sprawiedliwości w porozumieniu z Prokuratorem Generalnym określi, w drodze rozporządzenia, sposób dokonywania obliczeń i wzór formularza służącego do przekazywania danych, o których mowa w ust. 9, kierując się potrzebą przekazania opinii publicznej pełnej i rzetelnej informacji.
13. Pełnomocnik przekazuje corocznie do dnia 31 marca Prezesowi Urzędu Komunikacji Elektronicznej za pośrednictwem prokuratora który go powołał dane statystyczne niezbędne do wypełnienia obowiązku informacyjnego wobec Komisji Europejskiej.

Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz. U. z 1964 r. nr 43, poz. 296, z późn. zm.)

Po art. 232 dodaje się nowy art. 232a:

Dowód z pozyskania danych, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, z późn. zm.) może być przeprowadzony jedynie wyjątkowo, gdy ustalenie określonej okoliczności faktycznej za pomocą innego dowodu jest niemożliwe albo szczególnie utrudnione.

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. nr 171, poz. 1800, z późn. zm.)

W art. 180a ust. 1 pkt 1 słowa „okres 24 miesięcy” zastępuje się słowami „okres 12 miesięcy”.

Nadaje się nowe brzmienie art. 180g:

Podmioty, o których mowa w art. 180a ust. 1 pkt 2, w terminie do dnia 31 marca, składają Prezesowi UKE, za rok poprzedni informacje o:

- 1) liczbie przypadków, w których uzyskiwały od operatorów telekomunikacyjnych dane, o których mowa w art. 180c ust. 1;
 - 2) czasie, jaki upłynął między datą zatrzymania danych a datą złożenia przez podmioty, o których mowa w art. 180a ust. 1 pkt 2, wniosku lub ustnego żądania o ich udostępnienie;
 - 3) liczbie przypadków, w których wniosek lub ustne żądanie, o którym mowa w pkt 2, nie mógł być zrealizowany.
2. Prezes UKE przekazuje corocznie Komisji Europejskiej informacje, o których mowa w ust. 1.
3. Prezes Rady Ministrów określi, w drodze rozporządzenia, wzór formularza służącego do przekazywania informacji, o których mowa w ust. 1, Prezesowi UKE, kierując się potrzebą przekazania Komisji Europejskiej pełnej i rzetelnej informacji.