GIODO

Generalny Inspektor
Ochrony Danych Osobowych

ABC

zasad kontroli przetwarzania danych osobowych

BIURO GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH
ul. Stawki 2, 00-193 Warszawa
tel.: (22) 860 70 81
fax: (22) 860 70 86
kancelaria@giodo.gov.pl
www.giodo.gov.pl

Opracowanie: Bogusława Pilc –
Dyrektor Departamentu
Inspekcji Biura GIODO

© Copyright by GIODO

ISBN 978-83-7666-152-0

Druk: Wydawnictwo Sejmowe
Wydanie drugie poprawione
Warszawa, grudzień 2011

Spis treści

Wprowadzenie

Pojęcie „kontrola" należy do pojęć będących w powszechnym użyciu. Występuje ono w języku potocznym, publicystyce, piśmiennictwie naukowym. Należy również zauważyć, iż rozumienie tego pojęcia nie stwarza większych problemów i jego sens znaczeniowy pojmowany jest w sposób w miarę jednolity. Na potrzeby niniejszego opracowania istotne jest traktowanie kontroli jako funkcji.

Kontrola traktowana w kategoriach funkcjonalnych i przedmiotowych znajduje odzwierciedlenie w licznych definicjach formułowanych w doktrynie, zwłaszcza prawa administracyjnego, np. M. Jaroszyński określał kontrolę w sposób bardzo zwięzły, stwierdzając, iż jest nią – sprawdzenie stanu faktycznego (M. Jaroszyński, M. Zimmermann, W. Brzeziński, *Polskie prawo administracyjne, część ogólna*, Warszawa 1956, s. 440). Zdaniem E. Iserzona z kolei „kontrolą jest ogół czynności zmierzających do ustalenia faktycznego stanu rzeczy, połączony z porównaniem stanu istniejącego ze stanem planowanym" (E. Iserzon, *Prawo administracyjne*, Warszawa 1968, s. 174). W piśmiennictwie występują też bardziej rozbudowane definicje kontroli, np. J. Starościak przedstawiał, że kontrola polega na obserwowaniu, ustalaniu czy wykrywaniu stanu faktycznego, porównywaniu rzeczywistości z zamierzeniami, występowaniu przeciw zjawiskom niekorzystnym i sygnalizowaniu jednostkom kompetentnym dokonanych spostrzeżeń – bez decydowania jednak o zmianie kierunku działania jednostki skontrolowanej (J. Starościak, *Zarys nauki administracji*, Warszawa 1971, s. 356). Według W. Dawidowicza kontrolę można scharakteryzować jako działanie obejmujące: zbadanie istniejącego stanu rzeczy; zestawienie tego co istnieje, z tym co być powinno, co przewidują odpowiednie wzorce czy normy postępowania, i sformułowanie na tej podstawie odpowiedniej oceny; w przypadku rozbieżności między stanem faktycznym a stanem pożądanym – ustalenie przyczyn tych rozbieżności i sformułowanie zaleceń, mających na celu wskazanie sposobów usunięcia niepożądanych zjawisk ujawnionych przez kontrolę (W. Dawidowicz, *Zagadnienia ustroju administracji państwowej w Polsce*, Warszawa 1970, s. 34).

Biorąc pod uwagę powyższe poglądy oraz potoczne znaczenie słowa „kontrola", można stwierdzić, że kontrola jest funkcją, której istota tkwi w sprawdzaniu i ocenianiu określonej działalności. Prawo tworzy instytucje kontroli, które mają uprawnienia do podejmowania działań kontrolnych wobec określonego kręgu podmiotów, a podmioty te nie mogą się od kontroli uchylać. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (dalej: ustawa; tekst

jedn. Dz.U. z 2002 r. Nr 101, poz. 926 z późn. zm.) zobowiązuje Generalnego Inspektora Ochrony Danych Osobowych (dalej: Generalny Inspektor albo GIODO) do szeroko pojmowanych zadań kontrolnych w zakresie zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Realizowana przez Generalnego Inspektora funkcja kontrolna łączy się z możliwością władczego oddziaływania na podmioty kontrolowane. Działalność władcza – w przypadku naruszenia przepisów o ochronie danych osobowych – polega w szczególności na wydawaniu decyzji administracyjnych nakazujących przywrócenie stanu zgodnego z prawem.

Niniejsze opracowanie przedstawia podstawowe zasady wykonywania zadań kontrolnych GIODO – jako organu, który stoi na straży przysługującego każdemu prawa do ochrony danych osobowych.

I. Zadania kontrolne Generalnego Inspektora

Ustawa o ochronie danych osobowych w art. 12 pkt 1 wskazuje, iż do zadań Generalnego Inspektora Ochrony Danych Osobowych należy w szczególności „kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych". Przepisy te zawarte zostały w ustawie o ochronie danych osobowych oraz w wydanym na podstawie art. 39a ustawy – rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024; dalej: rozporządzenie).

Celem kontroli jest ustalenie stanu faktycznego w zakresie przestrzegania przez podmiot kontrolowany przepisów o ochronie danych osobowych oraz udokumentowanie dokonanych ustaleń.

Kontrole przeprowadzają inspektorzy w zespołach kontrolnych składających się najczęściej z trzech osób – dwóch pracowników (prawników) Departamentu Inspekcji Biura GIODO oraz jednego pracownika (informatyka) Departamentu Informatyki Biura GIODO. Czynności kontrolne „na miejscu" są dokonywane w siedzibie kontrolowanego podmiotu oraz w innym miejscu (np. jednostce organizacyjnej) wskazanym jako obszar przetwarzania danych osobowych. Kontroli poddawane są zarówno podmioty sektora publicznego, jak i podmioty prywatne, które w art. 3 ustawy zostały wskazane jako podmioty zobowiązane do ochrony danych osobowych – podmioty przetwarzające dane osobowe.

II. Zakres podmiotowy uprawnień kontrolnych Generalnego Inspektora

Zakres podmiotowy uprawnień kontrolnych Generalnego Inspektora jest bardzo szeroki. Jak już wskazano, kontroli poddawane są podmioty należące do sfery publicznej i prywatnej. Można dokonać podziału tych podmiotów, biorąc pod uwagę posiadanie przez nie statusu administratora danych, bądź brak takiego statusu. Kontrola przetwarzania danych osobowych obejmuje zarówno administratorów danych podlegających obowiązkowi zgłoszenia zbioru do rejestracji, jak też administratorów danych, którzy z mocy ustawy są z obowiązku rejestracji zwolnieni. Ponadto zauważyć należy, że w przypadku gdy administrator danych sam nie przetwarza danych, lecz zleca to innemu podmiotowi (zleceniobiorcy) w drodze umowy zawartej na piśmie, na zasadach określonych w art. 31 ustawy, kontroli podlega również ten podmiot (zleceniobiorca). Zatem obowiązki związane z kontrolą ciążą nie tylko na administratorze danych, lecz także – odpowiednio – na podmiocie zajmującym się przetwarzaniem danych na podstawie tzw. umowy powierzenia.

1. Podmioty publiczne

Zgodnie z art. 3 ust. 1 ustawa ma zastosowanie do organów państwowych, organów samorządu terytorialnego oraz do państwowych i komunalnych jednostek organizacyjnych. Podmioty te, jako należące do sektora publicznego, mogą decydować o celu i środkach przetwarzania danych w ramach zadań przyznanych im przepisami prawa. Kontrolą mogą być objęte np. Kancelaria Prezydenta RP, Kancelaria Sejmu, Kancelaria Senatu, Kancelaria Prezesa Rady Ministrów, ministerstwa, sądy, prokuratury, jednostki policji, urzędy skarbowe, publiczne zakłady opieki zdrowotnej, Zakład Ubezpieczeń Społecznych, gminy, powiaty, województwa i inne.

2. Podmioty prywatne

Drugą grupę podmiotów objętych kontrolą stanowią podmioty prywatne:

- podmioty niepubliczne realizujące zadania publiczne (np. prywatne zakłady opieki zdrowotnej, prywatne szkoły i przedszkola);
- osoby fizyczne i osoby prawne (np. spółki z o.o., spółki akcyjne, stowarzyszenia, fundacje, spółdzielnie) oraz jednostki organizacyjne niebędące osobami prawnymi (np. niemające osobowości prawnej spółki prawa handlowego); objęte są one zakresem stosowania ustawy, jeżeli przetwa-

rzają dane w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych (art. 3 ust. 2 pkt 2 ustawy).

Ustawa obejmuje te podmioty prywatne, które „mają siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej" (art. 3 ust. 3 ustawy). Podmioty te mogą realizować takie cele i stosować takie środki w zakresie przetwarzania danych osobowych, które w naturalny sposób wynikają ze specyfiki prowadzonej przez nie działalności.

3. Ograniczenia podmiotowe kontroli

Generalny Inspektor ma ograniczone prawo kontroli wobec następujących podmiotów:

- administratorów danych;
- administratorów danych dotyczących członków kościoła lub innego związku wyznaniowego o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby kościoła lub związku wyznaniowego;
- Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego – w odniesieniu do danych, które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy tych podmiotów.

Wobec wymienionych podmiotów Generalny Inspektor lub upoważnieni przez niego pracownicy Biura GIODO (inspektorzy) posiadają zredukowane uprawnienia kontrolne. W szczególności nie mają prawa:

- wstępu do pomieszczenia, w którym zlokalizowany jest zbiór danych oraz do pomieszczenia, w którym przetwarzane są dane poza zbiorem;
- przeprowadzania w pomieszczeniu kontrolowanego podmiotu niezbędnych badań lub innych czynności w celu oceny zgodności przetwarzania danych z ustawą;
- wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli;
- sporządzania kopii dokumentów i danych;
- przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych;
- zlecania sporządzania ekspertyz i opinii;

- wydawania decyzji administracyjnych, w tym decyzji nakazujących przywrócenie stanu zgodnego z prawem;
- rozpatrywania skarg w sprawach wykonania przepisów o ochronie danych osobowych;
- żądania wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień.

Wobec tych podmiotów Generalny Inspektor może jedynie żądać złożenia pisemnych lub ustnych wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego.

III. Zakres przedmiotowy uprawnień kontrolnych Generalnego Inspektora

Podczas kontroli przestrzegania przepisów o ochronie danych osobowych inspektor zwraca szczególną uwagę na następujące kwestie:

1. **Przesłanki legalności przetwarzania danych osobowych** – podmiot kontrolowany powinien wykazać co najmniej jedną z przesłanek legalności przetwarzania danych, które zostały wymienione w art. 23 ustawy. Gdy np. podstawą prawną przetwarzania danych jest zgoda osoby, której one dotyczą – inspektor żąda udokumentowania zgody; dowodem może być w szczególności oświadczenie na piśmie, nagranie bądź każdy inny nośnik informacji dokumentujący wyrażoną zgodę. Gdy z kolei dane są niezbędne do realizacji umowy, której dana osoba jest stroną – inspektor żąda przedstawienia treści tej umowy;
2. **Przesłanki legalności przetwarzania danych szczególnie chronionych** – podmiot kontrolowany jest obowiązany do przedstawienia dowodów legalności przetwarzania danych i wykazania, że spełnia co najmniej jedną z podstaw prawnych wymienionych w art. 27 ust. 2 ustawy. Gdy tą podstawą jest przepis szczególny innej ustawy, wówczas kontrolowany podmiot powinien precyzyjnie określić dany przepis – poprzez jego przedstawienie i podanie nazwy aktu prawnego, z którego pochodzi;
3. **Zakres i cel przetwarzania danych** – kontrolowany podmiot jest obowiązany podać kategorie osób (np. pracownicy, uczniowie, członkowie, klienci) oraz kategorie przetwarzanych danych i ich zakres (dane tzw.

zwykłe – np. imię, nazwisko, adres zamieszkania, data urodzenia, stan cywilny; dane szczególnie chronione i ich zakres – np. stan zdrowia, kod genetyczny, nałogi, pochodzenie rasowe, poglądy polityczne, religijne), a także wskazać cel, w jakim dane przetwarza (np. marketingowy, podatkowy, archiwalny);

4. **Merytoryczna poprawność danych i ich adekwatność do celu przetwarzania** – kontrolowany podmiot jest obowiązany wykazać merytoryczną poprawność, np. poprzez okazanie dokumentów, które potwierdzają poprawną pisownię kwestionowanego imienia, nazwiska czy daty urodzenia danej osoby. Badając adekwatność danych, inspektor szczegółowo analizuje wszystkie ich elementy oraz cel, w jakim są przetwarzane. Kontrolowany podmiot musi z kolei uzasadnić potrzebę posiadania danych osobowych – w stosunku do celu przetwarzania, w jakim je pozyskał (podmiot prywatny). W przypadku podmiotów publicznych wymagane jest podanie przepisu uprawniającego do przetwarzania określonych danych.
5. **Obowiązek informacyjny** – inspektor sprawdza, w jaki sposób jest realizowany obowiązek poinformowania każdej osoby, której dane dotyczą, tj. czy zakres informacji uwzględnia odrębnie uregulowane dwie sytuacje dotyczące źródła pozyskania danych (od osoby, której dane dotyczą – art. 24 ustawy, i nie od osoby, której dane dotyczą – art. 25), a zatem czy zawiera określone przepisami ustawy elementy, a ponadto czy poinformowanie ma indywidualny charakter i czy informacje zostały przedstawione w sposób zrozumiały dla odbiorcy;
6. **Zgłoszenie zbioru do rejestracji** – inspektor sprawdza, czy prowadzone przez podmiot kontrolowany zbiory danych nie podlegają w myśl art. 43 ust. 1 ustawy zwolnieniu z obowiązku rejestracji. Jeśli obowiązek rejestracji zaistniał i dokonano zgłoszenia zbiorów do rejestracji – badana jest bardzo szczegółowo treść wypełnionego formularza zgłoszenia (wzór został opublikowany w akcie wykonawczym do ustawy) oraz stan faktyczny odnoszący się do informacji podanych w zgłoszeniu. Inspektor ustala ponadto, czy ewentualna zmiana, w zakresie informacji podanych w zgłoszeniu, została Generalnemu Inspektorowi zgłoszona w terminie wskazanym w ustawie;
7. **Przekazywanie danych do państwa trzeciego** – inspektor sprawdza, czy kontrolowany podmiot uwzględnił co najmniej jedną z przesłanek wymienionych w art. 47 ustawy, zezwalających na legalne przekazanie danych poza obszar UE. Ponadto dokonuje oceny, czy zostały zastosowane odpowiednie środki techniczne i organizacyjne zabezpieczające dane, o których mowa w ustawie i rozporządzeniu;

8. **Powierzenie przetwarzania danych osobowych** (art. 31 ustawy) – inspektor sprawdza, czy umowa powierzenia została sporządzona na piśmie, a następnie szczegółowo bada jej treść; umowa powinna m.in. precyzyjnie określać zakres danych przekazanych do przetwarzania oraz podstawę i cel przetwarzania. Kopia umowy, potwierdzona za zgodność przez administratora danych, jest załączana do protokołu i szczegółowo opisywana. Ponadto może być przeprowadzona kontrola podmiotu, któremu zlecono przetwarzanie danych. W takim przypadku inspektor bada, czy dane są przetwarzane zgodnie z postanowieniami umowy powierzenia (w szczególności, jeśli chodzi o zakres danych i wskazany cel) oraz czy podmiot, któremu powierzono przetwarzanie danych, podjął środki zabezpieczające określone w przepisach o ochronie danych osobowych;
9. **Zabezpieczenie danych** – jednym z podstawowych celów kontroli jest sprawdzenie zgodności przetwarzania danych z przepisami o ochronie danych osobowych związanych z bezpieczeństwem przetwarzanych danych (rozdz. V ustawy oraz przywołane rozporządzenie Ministra Spraw Wewnętrznych i Administracji). Inspektor ocenia, czy administrator danych zgodnie z art. 36 ust. 1 ustawy zastosował środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych – odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności czy w odpowiedni sposób zabezpieczył dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem, lub zniszczeniem.

Przepisy o ochronie danych osobowych nie precyzują, jakimi środkami należy się posłużyć, aby zapewnić właściwą ochronę przetwarzania danych. O użyciu środków danego rodzaju decyduje administrator, a skuteczność zastosowanych rozwiązań podlega badaniom w czasie kontroli. Wymogi dotyczące zabezpieczenia danych odnoszą się zarówno do danych przetwarzanych w sposób tradycyjny, jak i do danych przetwarzanych w systemach informatycznych.

W toku kontroli ustala się, czy:

- wszystkie osoby biorące udział w procesie przetwarzania danych, tj. uczestniczące w jakichkolwiek operacjach wykonywanych na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie – posiadają upoważnienie nadane przez administratora danych (art. 37 ustawy);

- kontrolowany podmiot prowadzi ewidencję osób upoważnionych do przetwarzania danych (art. 39 ust. 1 ustawy), zawierającą:
  a) imię i nazwisko osoby upoważnionej,
  b) datę nadania upoważnienia,
  c) datę ustania upoważnienia,
  d) zakres upoważnienia,
  e) identyfikator, jeżeli dane przetwarzane są w systemie informatycznym;
- osoby upoważnione do przetwarzania danych zachowują te dane oraz sposób ich zabezpieczenia w tajemnicy (art. 39 ust. 2 ustawy);
- administrator danych wyznaczył administratora bezpieczeństwa informacji (art. 36 ust. 3 ustawy), tj. osobę lub osoby nadzorujące przestrzeganie zasad ochrony, chyba że sam sprawuje nadzór. Inspektor bada również, w jaki sposób jest wykonywany taki nadzór – m.in. czy zostały opracowane procedury określające obowiązki w tym zakresie, czy nadzór jest sprawowany sukcesywnie, w jakim przedziale czasowym, czy obejmuje wszystkie zagadnienia dotyczące zastosowanych zabezpieczeń i czy jest skuteczny;
- administrator danych zapewnił kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane (udostępniane) – art. 38 ustawy. Inspektor bada również sposób sprawowania takiej kontroli;
- urządzenia i systemy informatyczne spełniają wymogi bezpieczeństwa. Ocenę bezpieczeństwa rozpoczyna inspektor od analizy dokumentów określających politykę bezpieczeństwa kontrolowanego podmiotu w zakresie ochrony fizycznej obiektów, kontroli dostępu do poszczególnych systemów informatycznych i usług sieciowych oraz w zakresie ochrony zasobów informatycznych przed nieuprawnionym dostępem, przejęciem lub zniszczeniem przy użyciu szkodliwego programowania i narzędzi (tzw. wirusy, robaki, konie trojańskie, rootkity itp.).

Elementy kontroli urządzeń i systemów informatycznych:

1) bezpieczeństwo fizyczne – podstawowymi elementami oceny są: sposób zabezpieczenia obiektów i pomieszczeń, gdzie znajdują się systemy informatyczne i nośniki informacji, na których przechowywane są kopie zapasowe lub archiwalne danych, oraz pomieszczeń, gdzie zlokalizowane są urządzenia sieciowe, serwery i stacje robocze. Pomieszczenia takie, zgodnie z wymaganą polityką bezpieczeństwa, powinny być wskazane

jako obszar przetwarzania danych (§ 4 pkt 1 rozporządzenia). Inspektor – dokonując oceny – sprawdza m.in.:

- formę realizacji ochrony fizycznej z udziałem czynnika ludzkiego (np. system organizacji służby ochrony),
- budowlane urządzenia zabezpieczające (np. drzwi stalowe, kraty stalowe, rolety przeciwwłamaniowe, okiennice i szyby zabezpieczające otwory okienne),
- urządzenia fizycznej kontroli dostępu do pomieszczeń (np. zamki, kłódki, zasuwy, blokady),
- elektroniczne urządzania zabezpieczające przed włamaniem i pożarem (np. sygnalizacja włamania lub napadu, sygnalizacja pożaru, system wideo nadzoru),
- elektroniczny system kontroli dostępu, z rejestracją operacji otwierania i zamykania pomieszczeń przez osoby uprawnione.

Stosowanie któregokolwiek z wymienionych środków powinno być uzależnione od występujących zagrożeń – w zakresie zapewnienia poufności, integralności i tzw. rozliczalności przetwarzanych danych;

2) bezpieczeństwo systemów informatycznych – przed przystąpieniem do kontroli inspektor zapoznaje się z architekturą używanych systemów oraz lokalizacją i strukturą prowadzonych zbiorów danych. Podstawowym dokumentem wymaganym od kontrolowanego podmiotu jest polityka bezpieczeństwa (§ 3 rozporządzenia), która zgodnie z § 4 pkt 2–4 rozporządzenia powinna zawierać:
   - wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych;
   - opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
   - sposób przepływu danych pomiędzy poszczególnymi systemami.

Na podstawie uzyskanych informacji, ustalonych kategorii danych oraz sposobu korzystania ze środków teletransmisji – inspektor ocenia poziom bezpieczeństwa, jaki powinien być zastosowany: podstawowy, podwyższony bądź wysoki.

Zgodnie z § 6 rozporządzenia, wyróżniającym poziomy bezpieczeństwa przetwarzania danych osobowych, przyjmuje się, że:

- **poziom co najmniej podstawowy stosuje się, gdy:**

„1) w systemie informatycznym nie są przetwarzane dane, o których mowa w art. 27 ustawy,

oraz

2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną" (§ 6 pkt 2);

- **poziom co najmniej podwyższony stosuje się, gdy:**

„1) w systemie informatycznym przetwarzane są dane osobowe, o których mowa w art. 27 ustawy,

oraz

2) żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną" (§ 6 pkt 3);

- **poziom wysoki stosuje się**, „gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną" (§ 6 pkt 4).

Ostatnim etapem kontroli bezpieczeństwa systemów jest szczegółowe sprawdzenie stosowanych procedur zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz kontrola zastosowanych środków bezpieczeństwa. Dokumentem, który na tym etapie kontroli inspektor wnikliwie analizuje, jest wskazana w § 3 rozporządzenia instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, która zgodnie z § 5 rozporządzenia powinna określać:

„1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;

2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;

3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;

5) sposób, miejsce i okres przechowywania;

a) elektronicznych nośników informacji zawierających dane osobowe,

b) kopii zapasowych, o których mowa w pkt 4;

6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia [tj. oprogramowania szkodliwego];

7) sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 [rozporządzenia, tj. dotyczących rejestracji informacji, kto, kiedy i jakie dane wprowadzał do systemu, z jakiego źródła dane te pochodziły oraz kiedy i jakim odbiorcom były udostępniane];

8) procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych".

Podkreślenia wymaga, że inspektor w toku czynności kontrolnych weryfikuje zarówno treść instrukcji, jak również sprawdza, czy deklarowane procedury oraz środki ochrony są rzeczywiście stosowane. Badany jest mechanizm logowania i uwierzytelnienia się użytkownika każdego systemu czy też modułu programowego oraz system kontroli uprawnień. W sytuacji, gdy zakres przetwarzanych danych wymaga stosowania różnych poziomów uprawnień dla poszczególnych grup użytkowników – ocenie poddawane są mechanizmy, które kontrolę taką umożliwiają.

W przypadku systemów teleinformatycznych szczegółowej kontroli poddawane są zastosowane mechanizmy ochrony teletransmisji. Podstawowym wymogiem jest zabezpieczenie informacji przesyłanych drogą teletransmisji – przed udostępnieniem ich osobom nieuprawnionym oraz przed utratą, uszkodzeniem lub zniszczeniem danych. Podczas kontroli zastosowanych w tym zakresie rozwiązań brane są pod uwagę przyjęte środki ochrony kryptograficznej, jak również sposób zarządzania kluczami kryptograficznymi i hasłami. W przypadku, gdy kontrolowany podmiot wykorzystuje do przetwarzania danych komputery przenośne lub do przekazywania danych poza swoją siedzibę korzysta z elektronicznych nośników informacji – przedmiotem kontroli jest sposób ich kryptograficznego zabezpieczenia.

Elementem kontroli bezpieczeństwa systemów teleinformatycznych jest także ich funkcjonalność. Zgodnie bowiem z § 7 rozporządzenia przedmiotem szczegółowej kontroli w tym zakresie jest ustalenie, czy:

„1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie – system ten zapewnia odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu;

2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

3) źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą;

4) informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

5) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i pkt 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.

4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu".

IV. Rodzaje kontroli

Kontrola z urzędu – wykonywana z inicjatywy własnej Generalnego Inspektora. Stanowi ona konsekwencję obowiązku zrealizowania zadań kontrolnych nałożonych przez ustawę, w szczególności w toku postępowań rejestracyjnych prowadzonych przez Departament Rejestracji Zbiorów Danych Osobowych oraz w toku rozpatrywania skarg dokonywanych przez Departament Legislacji, Orzecznictwa i Skarg.

Kontrola na wniosek – pozostaje również w sferze wykonywania zadań kontrolnych przez Generalnego Inspektora, natomiast inspiracja do podjęcia i prowadzenia określonej kontroli pochodzi z zewnątrz, od innego podmiotu (np. Najwyższej Izby Kontroli, Państwowej Inspekcji Pracy, prokuratury, związków zawodowych, pracodawców, osoby fizycznej).

Kontrola kompleksowa – dotyczy wszystkich zbiorów danych osobowych prowadzonych przez kontrolowanego administratora danych oraz obejmuje swoim zakresem wszystkie wymogi określone w przepisach o ochronie danych osobowych, mające zastosowanie w działalności danego podmiotu.

Kontrola częściowa – dotyczy zwykle poszczególnych zagadnień w procesie przetwarzania danych będących przedmiotem skargi, takich jak legalność pozyskiwania danych skarżącego, sposób dopełnienia obowiązku informacyjnego wobec skarżącego, czy też problemów pojawiających się w toku postępowań rejestracyjnych, np. podstawy prawnej, zakresu danych, celu przetwarzania danych – czyli zgodności informacji podanych w zgłoszeniu zbioru ze stanem faktycznym. Przedmiotem kontroli może też być wyłącznie kwestia zabezpieczenia danych osobowych, dopełnienie obowiązku rejestracyjnego lub tym podobne.

Kontrola sektorowa – kompleksowa lub częściowa – wskazana w rocznym harmonogramie kontroli, dotycząca wybranej kategorii podmiotów lub zagadnień.

V. Uprawnienia inspektora ochrony danych osobowych

W celu wykonania zadań w zakresie kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych, Generalny Inspektor, zastępca Generalnego Inspektora lub upoważnieni przez niego inspektorzy wyposażeni zostali w szerokie kompetencje do podejmowania określonych czynności kontrolnych (art. 14 ustawy). Zatem uprawnienie do kontroli wynika bezpośrednio z ustawy o ochronie danych osobowych. Zasadą jest, że kontrole, prowadzane przez inspektorów upoważnionych przez Generalnego Inspektora lub jego zastępcę, są zazwyczaj zapowiadane z kilkudniowym wyprzedzeniem. Podmioty, które mają być poddane kontroli, informowane są w pierwszej kolejności telefonicznie, a następnie na piśmie (faksem) przedstawiany jest ogólny przedmiot kontroli, termin dokonania czynności oraz prośba o przygotowanie dokumentacji dotyczącej przetwarzania danych. Odpowiednie przygotowanie się danego podmiotu do kontroli GIODO istotnie wpływa na zapewnienie sprawnego jej przebiegu, co ma znaczenie zarówno dla tego podmiotu, jak i dla inspektorów. Kontrola trwa zwykle kilka dni, jednak jeśli dotyczy dużych podmiotów, może zająć i kilka tygodni.

Zgodnie z ustawą inspektorzy przeprowadzają czynności kontrolne w godzinach od 6.00 do 22.00. W praktyce zazwyczaj umawiają się z kontrolowanym w godzinach pracy, np. między 8.00 a 16.00. Zdarza się jednak, że ze względu na okoliczności sprawy czynności są dokonywane w innych godzinach, np. od 9.00 do 18.00 lub dłużej.

1. Legitymacja i upoważnienie.

Kontrolę przeprowadza się wyłącznie po okazaniu legitymacji służbowej inspektora Biura GIODO oraz upoważnienia imiennego, których wzór określony został w załącznikach do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. nr 94, poz. 923 z późn. zm.) zmienionego rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 11 maja 2011 r. zmieniającym rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. Nr 103, poz. 601).

Opis wzoru legitymacji inspektora GIODO
awers legitymacji:
- legitymacja koloru niebieskiego,
- napisy w kolorze czarnym: Rzeczpospolita Polska, Biuro Generalnego Inspektora Ochrony Danych Osobowych,
- numer legitymacji,
- orzeł z godła RP,
- pasek przekątny koloru biało-czerwonego;

rewers legitymacji:
- legitymacja koloru niebieskiego,
- napisy w kolorze czarnym: LEGITYMACJA SŁUŻBOWA Inspektora Ochrony Danych Osobowych ważna do..., miejsce na fotografię, miejsce na pieczęć, nazwisko, imię, nr ewidencyjny PESEL, (podpis wystawcy), (podpis właściciela),
- hologram z literami w kolorze niebieskim;

wymiary legitymacji:
- wysokość legitymacji 90 mm,
- szerokość legitymacji 65 mm,
- wysokość fotografii 35 mm,
- szerokość fotografii 25 mm;

rodzaj papieru i zabezpieczeń:
- gramatura papieru 200,
- papier kredowany dwustronnie – matowy,
- hologram,
- w miejscach wpisu nazwiska i imienia oraz numeru ewidencyjnego PESEL nadruk cienkich linii zabezpieczających.

Wzór
upoważnienia imiennego do przeprowadzenia czynności kontrolnych

.....
(pieczęć podłużna Generalnego Inspektora
Ochrony Danych Osobowych)

L.dz. .....

Upoważnienie imienne

Na podstawie art. 12 pkt 1 i 2 w związku z art. 14 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271,

z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238 oraz z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228 i Nr 229, poz. 1497)

upoważniam

Panią/Pana .....

(imię i nazwisko inspektora)

stanowisko służbowe .....

nr legitymacji służbowej .....

do przeprowadzenia kontroli:

.....

.....

.....

.....

(określenie: podmiotu objętego kontrolą albo zbioru danych, albo miejsca poddawanego kontroli)

w zakresie:

.....

.....

.....

.....

(określenie zakresu przedmiotowego kontroli)

Data rozpoczęcia kontroli: .....

Przewidywany termin zakończenia kontroli: .....

Upoważnienie jest ważne jedynie z równoczesnym okazaniem legitymacji służbowej.

.....

(miejsce i data wystawienia upoważnienia)

pieczęć urzędowa

.....

(podpis Generalnego Inspektora Ochrony Danych Osobowych)

Pouczenie kontrolowanego podmiotu o jego prawach i obowiązkach

1. Zgodnie z art. 15 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych osobowych są obowiązani umożliwić inspektorowi przeprowadzenie kontroli, a w szczególności umożliwić przeprowadzenie czynności oraz spełnić żądania, o których mowa w art. 14 pkt 1–4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, polegające na:

- umożliwieniu wstępu inspektorom, w godzinach od 6.00 do 22.00, za okazaniem niniejszego imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym jest zlokalizowany zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą o ochronie danych osobowych,
- żądaniu złożenia pisemnych lub ustnych wyjaśnień oraz wzywania i przesłuchiwania osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
- umożliwieniu wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,
- przeprowadzaniu oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

2. Zgodnie z art. 16 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, z czynności kontrolnych inspektor sporządza protokół, którego jeden egzemplarz doręcza kontrolowanemu administratorowi danych. Protokół podpisują inspektor i kontrolowany administrator danych, który może wnieść do protokołu umotywowane zastrzeżenia i uwagi (art. 16 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych). W razie odmowy podpisania protokołu przez kontrolowanego administratora danych inspektor czyni o tym wzmiankę w protokole, a odmawiający podpisu może, w terminie 7 dni, przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi (art. 16 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych).

.....
(data i czytelny podpis osoby
reprezentującej kontrolowany podmiot)

Inspektorzy przedstawiają kontrolowanemu administratorowi wskazane dokumenty przed podjęciem czynności kontrolnych. Wystawcą ich jest Generalny Inspektor lub jego zastępca.

2. Termin i czas kontroli

Inspektorzy Biura GIODO są uprawnieni do przeprowadzenia, bez uprzedzenia w godzinach od 6.00 do 22.00 kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Termin kontroli jest ustalany przez GIODO. Przepisy ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz.U. z 2007 r. Nr 155 poz. 1095) wprowadzają limity czasowe w odniesieniu do kontroli odbywających się u przedsiębiorców (art. 83 ust. 1). Przy ustalaniu terminu i czasu uwzględnia się w szczególności rodzaj kontroli (kompleksowa, częściowa), zakres przedmiotowy kontroli i wielkość podmiotu kontrolowanego. Czas trwania czynności może w ich toku ulec skróceniu lub przedłużeniu – w zależności od okoliczności danej kontroli.

3. Miejsce kontroli

Kontrolę przeprowadza się w siedzibie podmiotu kontrolowanego oraz w innych miejscach wykonywania przez niego zadań w procesie przetwarzania danych, w tym w miejscu przechowywania dokumentacji zawierającej dane osobowe.

Przed podjęciem czynności kontrolnych inspektorzy Biura GIODO zgłaszają swoją obecność kontrolowanemu.

4. Wstęp do pomieszczeń, w których przetwarzane są dane osobowe

W ramach powyższego uprawnienia inspektor ma prawo wstępu na teren kontrolowanego podmiotu oraz do pomieszczeń, w których zlokalizowany jest zbiór danych, oraz do pomieszczeń, w których przetwarzane są dane poza zbiorem. Jest uprawniony również do przeprowadzania oględzin budynków, pomieszczeń lub części pomieszczeń, stanowisk pracy tworzących obszar, w którym przetwarzane są dane osobowe, jak też przeprowadzania oględzin przebiegu procesu ich przetwarzania. Ponadto inspektor ma prawo dokonywania niezbędnych badań lub innych czynności kontrolnych – w celu oceny zgodności przetwarzania danych z ustawą.

5. Żądanie pisemnych lub ustnych wyjaśnień

Inspektor może zażądać złożenia pisemnych lub ustnych wyjaśnień w kwestiach objętych kontrolą, zarówno od podmiotu kontrolowanego, jak i od wszystkich osób, które wykonują na rzecz tego podmiotu jakiekolwiek operacje na danych osobowych, m.in. takie, jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zwłaszcza operacje w systemach informatycznych. Kontrolujący inspektor decyduje o tym, które osoby okażą się niezbędne, aby wyjaśnić stan faktyczny. Zasadą jest, że w pierw-

szej kolejności wyjaśnienia składa administrator danych, który opisuje poszczególne etapy procesu przetwarzania danych. Następnie informacje przekazują pozostałe osoby biorące bezpośredni udział w tym procesie.

6. Wzywanie i przesłuchiwanie osób

Inspektor ma prawo wzywać i przesłuchiwać osoby w związku z przeprowadzaną kontrolą. Może to być każda osoba, która posiada określoną wiedzę na temat okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy. Przesłuchanie osób w charakterze świadka następuje zwykle podczas badania legalności przetwarzania danych oraz w sytuacji, gdy inne środki dowodowe okazały się niewystarczające do ustalenia stanu faktycznego.

7. Wgląd do dokumentów i sporządzanie ich kopii

Korzystając ze swych uprawnień, inspektor może żądać okazania wszelkich dokumentów i danych mających bezpośredni związek z przedmiotem kontroli, takich jak statut, pozwolenie na prowadzenie określonej działalności, regulamin organizacyjny, instrukcja kancelaryjna, wypis z Krajowego Rejestru Sądowego, umowy (np. umowa powierzenia), decyzje, postanowienia, zarządzenia i inne dokumenty określające procedury dotyczące ocenianego procesu przetwarzania danych. Ponadto inspektor żąda przedstawienia dokumentacji, której opracowanie jest obowiązkowe, tj. polityki bezpieczeństwa, instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz ewidencji osób upoważnionych do przetwarzania danych. Inspektor ma także prawo sporządzania kopii wskazanych dokumentów, niezbędnych dla celów kontroli.

8. Oględziny urządzeń, nośników oraz systemów informatycznych

W czasie kontroli inspektor może dokonać oględzin urządzeń, elektronicznych nośników informacji zawierających dane osobowe oraz systemu informatycznego. Wykonując te czynności, inspektorzy biorą pod uwagę w szczególności lokalizację sprzętu oraz zastosowane środki zapewnienia poufności, integralności i rozliczalności danych (§ 2 pkt 7, 8 i 10 rozporządzenia), jak też zapewnienie funkcjonalności systemów informatycznych.

9. Zlecanie ekspertyz i opinii

Gdy w trakcie kontroli inspektor napotka szczególnie skomplikowane kwestie, wymagające specjalistycznej wiedzy lub zastosowania odpowiedniego sprzętu, jest uprawniony do zamówienia ekspertyzy czy też opinii na ten temat. W praktyce są to zwykle rzadkie przypadki i mają charakter wyjątkowy.

VI. Organizacja kontroli

W celu przeprowadzenia wszystkich niezbędnych czynności kontrolnych w sposób zgodny z prawem, zapewnienia sprawnego ich przebiegu oraz podjęcia wszelkich działań niezbędnych do dokładnego wyjaśnienia stanu faktycznego inspektorzy podejmują określone działania przygotowawcze.

1. Zebranie materiałów dotyczących kontroli

Przed podjęciem czynności kontrolnych inspektorzy wnikliwie przygotowują informacje dotyczące podmiotów, wobec których będą prowadzone kontrole. W tym celu m.in. zapoznają się ze wszelkimi materiałami będącymi w dyspozycji statutowych jednostek organizacyjnych Biura GIODO, głównie Departamentu Orzecznictwa, Legislacji i Skarg oraz Departamentu Rejestracji Zbiorów Danych Osobowych. Jednocześnie pozyskują informacje dostępne w Internecie i innych mediach. Analizują również przepisy, na podstawie których działa dany podmiot, a także orzecznictwo w zakresie problemów stanowiących przedmiot kontroli.

2. Opracowanie planu kontroli

W celu wyznaczenia zakresu przedmiotowego kontroli, opracowywany jest projekt upoważnienia do przeprowadzenia kontroli, który jest zatwierdzany przez Generalnego Inspektora lub jego zastępcę, zawierający m.in. oznaczenie podmiotu objętego kontrolą albo zbioru danych, albo miejsca poddawanego kontroli, szczegółowy zakres kontroli, datę rozpoczęcia i przewidywany termin zakończenia kontroli.

VII. Przebieg kontroli

Celem kontroli, jak już wskazywano, jest ustalenie stanu faktycznego w zakresie przestrzegania przez podmiot kontrolowany przepisów o ochronie danych osobowych oraz udokumentowanie dokonanych ustaleń. Uczestnikami procesu kontroli jest organ kontrolny GIODO oraz podmiot kontrolowany. Ustawa o ochronie danych osobowych wskazuje prawa i obowiązki uczestników, które mają zapewnić osiągnięcie celu kontroli.

1. Obowiązki inspektora

Inspektor przeprowadzający kontrolę jest zobowiązany do przestrzegania uprawnień, które przysługują kontrolowanemu podmiotowi. Zapoznanie kon-

trolowanego z jego prawami i obowiązkami następuje poprzez przedstawienie mu upoważnienia do kontroli zawierającego pouczenie kontrolowanego podmiotu o jego prawach i obowiązkach. Osoba uprawniona do reprezentacji tego podmiotu poświadcza zapoznanie się z pouczeniem poprzez złożenie pod nim podpisu. Inspektor ma obowiązek poinformować, w jaki sposób kontrolowany może domagać się np. wniesienia uwag, zastrzeżeń, poprawek i sprostowań do protokołu kontroli. W żadnym wypadku inspektor nie może przekraczać zakresu upoważnienia udzielonego przez Generalnego Inspektora – nie może domagać się okazania dokumentów lub podawać informacji o okolicznościach, które nie mają związku z przedmiotem kontroli, np. dotyczących sytuacji finansowej. W swoim działaniu powinien wykazać się obiektywizmem oraz zachować w tajemnicy informacje, które uzyskał w związku z wykonywaniem obowiązków służbowych.

2. Obowiązki kontrolowanego

Kontrolowany ma obowiązek umożliwić inspektorowi przeprowadzenie czynności kontrolnych oraz powinien udostępnić wszelkie żądane dokumenty i nośniki informacji związane z zakresem kontroli. Na żądanie inspektora kontrolowany jest obowiązany wydać kopie wskazanych dokumentów oraz tzw. zrzuty (wydruki) z ekranu komputera. Powinien czynnie uczestniczyć w prowadzonej kontroli: udzielać wyjaśnień, zapewnić terminowe udzielanie informacji przez podległych pracowników i inne osoby uczestniczące w procesie przetwarzania danych, być do dyspozycji w czasie trwania kontroli – w celu zapewnienia sprawnego jej przebiegu.

VIII. Dokumentowanie czynności kontrolnych

Poszczególne czynności kontrolne są dokumentowane (utrwalane) w celu włączenia ich do materiału dowodowego, na podstawie którego ustalany jest stan faktyczny. Inspektorzy sporządzają z poszczególnych czynności kontrolnych protokoły, które stanowią załączniki do protokołu kontroli.

1. Rodzaje protokołów z poszczególnych czynności
   1) Protokół przyjęcia ustnych wyjaśnień – zawiera oznaczenie organu kontroli i jego siedziby, wskazanie wykonującego tę czynność inspektora (imię, nazwisko, stanowisko służbowe, numer legitymacji służbowej i upoważnienia), podstawy prawnej uprawniającej do przyjęcia wyjaśnień (art. 14 pkt 2 ustawy), wskazanie osoby składającej wyjaśnienia (imię, nazwisko i stanowisko), treść złożonych

wyjaśnień, datę sporządzenia protokołu, podpis osoby składającej wyjaśnienia i podpis inspektora przyjmującego wyjaśnienia.

2) Protokół przesłuchania świadka – zawiera oznaczenie organu kontroli i jego siedziby, wskazanie wykonującego tę czynność inspektora (imię, nazwisko, stanowisko służbowe, numer legitymacji służbowej i upoważnienia), podstawy prawnej uprawniającej do przesłuchania (art. 14 pkt 2 ustawy), pouczenie świadka o jego prawach i obowiązkach, wskazanie osoby przesłuchiwanej (imię, nazwisko, adres, miejsce pracy, stanowisko służbowe), datę sporządzenia protokołu, podpis osoby przesłuchiwanej i podpis inspektora przesłuchującego.

3) Protokół oględzin – zawiera oznaczenie organu kontroli i jego siedziby, oznaczenie przedmiotu oględzin (np. miejsca, pomieszczeń, dokumentów, urządzeń, nośników informacji, systemów informatycznych), podstawę prawną uprawniającą do przeprowadzenia oględzin (art. 14 pkt 4 ustawy), wskazanie wykonującego tę czynność inspektora (imię, nazwisko, stanowisko służbowe), wskazanie osób uczestniczących w oględzinach (imię, nazwisko, zajmowane stanowisko służbowe), datę i miejsce oględzin, szczegółowe ustalenia, sposób utrwalenia stanu w toku oględzin, podpisy osób uczestniczących w czynności oględzin, podpisy inspektora.

2. Protokół kontroli zawiera elementy wskazane w art. 16 ust. 1a ustawy:
   1) nazwę podmiotu kontrolowanego w pełnym brzmieniu i jego adres;
   2) imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia inspektora;
   3) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot;
   4) datę rozpoczęcia i zakończenia czynności kontrolnych, z wymienieniem dni przerw w kontroli;
   5) określenie przedmiotu i zakresu kontroli;
   6) opis stanu faktycznego stwierdzonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
   7) wyszczególnienie załączników stanowiących składową część protokołu;
   8) omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień;
   9) parafy inspektora i osoby reprezentującej podmiot kontrolowany na każdej stronie protokołu;
   10) wzmiankę o doręczeniu egzemplarza protokołu osobie reprezentującej podmiot kontrolowany;

11) wzmiankę o wniesieniu lub niewniesieniu zastrzeżeń i uwag do protokołu;
12) datę i miejsce podpisania protokołu przez inspektora oraz przez osobę lub organ reprezentujący podmiot kontrolowany.

Załącznikami do protokołu kontroli są protokoły z poszczególnych czynności oraz inne dowody związane z kontrolą.

Protokół kontroli jest sporządzany przez inspektorów w dwóch jednobrzmiących egzemplarzach, z których jeden doręcza się kontrolowanemu podmiotowi lub osobie przez niego upoważnionej. Drugi egzemplarz pozostaje w aktach kontroli. Kontrolowany ma prawo wnieść na piśmie umotywowane zastrzeżenia i uwagi – zarówno do treści, jak i do ustaleń zawartych w protokole. Inspektor jest obowiązany rozpatrzyć złożone zastrzeżenia i uwagi oraz ustosunkować się do nich. O sposobie rozpatrzenia tych kwestii kontrolowany podmiot informowany jest na piśmie.

Gdy kontrolowany podmiot odmówi podpisania protokołu, inspektor czyni o tym wzmiankę w protokole kontroli. Kontrolowany może w terminie 7 dni, od dnia przedstawienia protokołu, przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi.

3. Wnioski z kontroli

Na podstawie zebranego w toku kontroli materiału dowodowego inspektor przedstawia wnioski z kontroli. Jeżeli na podstawie wyników kontroli inspektor stwierdzi naruszenie przepisów o ochronie danych osobowych, występuje do Generalnego Inspektora o zastosowanie środków określonych w ustawie o ochronie danych osobowych.

IX. Uprawnienia pokontrolne

Ustawa o ochronie danych osobowych wyraźnie określa, jakie środki przysługują Generalnemu Inspektorowi, gdy naruszone zostaną przepisy o ochronie danych osobowych.

1. Wszczęcie postępowania

Na podstawie wyników kontroli następuje wszczęcie postępowania administracyjnego (art. 61 § 4 k.p.a.). Zawiadomienie o wszczęciu postępowania przesyłane jest kontrolowanemu podmiotowi; zawiera ono m.in. wyszczególnienie

stwierdzonych w toku kontroli uchybień, dotyczących przedmiotu postępowania. W zawiadomieniu podane są przepisy o ochronie danych osobowych, które zostały naruszone (uzasadnienie prawne), oraz opis stanu faktycznego ze wskazaniem dowodów, na podstawie których został on ustalony (uzasadnienie faktyczne). Ponadto kontrolowany podmiot jest informowany o prawie złożenia dodatkowych wyjaśnień i o prawie przesłania uzupełniających dowodów (np. dokumentów lub wydruków z systemu informatycznego), potwierdzających usunięcie stwierdzonych uchybień. Jednocześnie jest określony termin, w jakim może nastąpić realizacja tego prawa. W sytuacji, gdy kontrolowany nie skorzysta z przysługującego mu uprawnienia, decyzja kończąca postępowanie zostanie wydana na podstawie materiału dowodowego zebranego w toku kontroli, o czym również informowany jest kontrolowany podmiot.

2. Rodzaje decyzji

W wyniku przeprowadzonej kontroli Generalny Inspektor wydaje decyzje:

1) nakazującą przywrócenie stanu zgodnego z prawem, jeżeli zostały naruszone przepisy o ochronie danych osobowych (treść nakazu wynika z art. 18 ustawy);

lub

2) umarzającą postępowanie jako bezprzedmiotowe, jeżeli postępowanie administracyjne zostało wszczęte w wyniku stwierdzonych w toku kontroli uchybień, a w trakcie postępowania kontrolowany podmiot je usunął i przywrócił stan zgodny z prawem.

Jeżeli kontrolowany podmiot kwestionuje skierowaną do niego decyzję, może zwrócić się do Generalnego Inspektora z wnioskiem o ponowne rozpatrzenie sprawy (art. 21 ust. 1 ustawy). Na decyzję Generalnego Inspektora wydaną w przedmiocie wniosku o ponowne rozpatrzenie sprawy przysługuje kontrolowanemu skarga do sądu administracyjnego (art. 21 ust. 2 ustawy). W pozostałym zakresie obowiązują przepisy kodeksu postępowania administracyjnego.

3. Wniosek o wszczęcie postępowania dyscyplinarnego

Na podstawie ustaleń kontroli inspektor może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień. Kontrolowany podmiot jest obowiązany do poinformowania Generalnego Inspektora w określonym terminie o wynikach tego postępowania i podjętych działaniach (art.17 ust. 2 ustawy). W praktyce Generalny Inspektor kieruje do wskazanego podmiotu wniosek za-

wierający m.in. wskazanie osób, wobec których żądanie wszczęcia postępowania jest kierowane. Jednocześnie przedstawia zebrane w trakcie kontroli dowody świadczące o winie tych osób i żąda w oznaczonym terminie przedstawienia rozstrzygnięcia.

4. Zawiadomienie o popełnieniu przestępstwa

Jeżeli wyniki kontroli będą wskazywać, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej wyczerpuje znamiona przestępstwa określonego w art. 49, art. 51, art. 52, art. 53, art. 54 lub art. 54a ustawy, wówczas Generalny Inspektor jest obowiązany skierować zawiadomienie o popełnieniu przestępstwa do organu powołanego do ścigania przestępstw. Do zawiadomienia dołączane są dowody zgromadzone w toku czynności kontrolnych, dokumentujące podejrzenie popełnienia wskazanego czynu zabronionego. Materiał dowodowy, będący podstawą skierowania zawiadomienia, jest zatem pozyskiwany przez inspektorów w wyniku przeprowadzenia bezpośredniej i szczegółowej kontroli wobec podmiotu przetwarzającego dane osobowe.

Wybrane pytania i odpowiedzi

Czy kontrola u administratora danych powinna być wcześniej zapowiedziana?

Ustawa o ochronie danych osobowych nie reguluje tej kwestii. Jednak przyjąć należy, iż administrator danych, u którego będą prowadzone czynności kontrolne, powinien być poinformowany o terminie kontroli. Kontrolowany podmiot ma wówczas możliwość przygotowania się do kontroli, a w szczególności sprawdzenia dokumentacji, uzupełnienia ewentualnych nieprawidłowości, które mogłyby zostać zakwestionowane przez inspektora. Może również podjąć odpowiednie działania organizacyjne, które pozwolą na usprawnienie i przyspieszenie przeprowadzenia czynności kontrolnych. Zaznaczyć należy, że inspektor może przeprowadzić kontrolę bez uprzedzenia, jeżeli okoliczności sprawy wskazują, iż kontrolowany mógłby ukryć dowody, które świadczą o popełnieniu przez niego czynu zabronionego wskazanego w ustawie. Jednakże w odniesieniu do przedsiębiorców obowiązują regulacje dotyczące zawiadomienia o kontroli. Stosownie do art. 79 ust. 4 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz.U. z 2007 r. Nr 155 poz. 1095) kontrolę wszczyna

się nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomienia o zamiarze wszczęcia kontroli.

Czy inspektor może wykonywać czynności kontrolne wyłącznie na podstawie legitymacji służbowej?

Inspektor nie jest uprawniony do wykonywania czynności kontrolnych, jeżeli okaże wyłącznie legitymację służbową. Zgodnie z art. 14 pkt 1 ustawy inspektor przeprowadzający kontrolę jest obowiązany przedstawić kontrolowanemu podmiotowi również upoważnienie imienne wystawione przez Generalnego Inspektora lub jego zastępcę.

Czy w toku kontroli mogą być wzywani i przesłuchiwani w charakterze świadka pracownicy podmiotu kontrolowanego?

Tak. Inspektor może w czasie trwania postępowania kontrolnego wzywać i przesłuchiwać osoby, w myśl art. 14 pkt 2 ustawy, w zakresie niezbędnym do ustalenia stanu faktycznego. Zatem pracownicy kontrolowanego podmiotu są obowiązani złożyć zeznania w sprawie prowadzonej przez inspektora kontroli.

W jakim terminie inspektor może przedstawić kontrolowanemu administratorowi danych protokół kontroli?

Ustawodawca nie wskazuje terminu do przedstawienia kontrolowanemu administratorowi danych protokołu kontroli. W praktyce dokument ten jest przedstawiany niezwłocznie po zakończeniu wszystkich czynności związanych z kontrolą. Na termin ma wpływ w szczególności zakres kontroli, wielkość podmiotu kontrolowanego oraz charakter danej sprawy. Gdy np. sprawa jest szczególnie skomplikowana, protokół kontroli jest doręczany w terminie późniejszym.

Kto jest uprawniony do podpisania protokołu kontroli?

Protokół kontroli podpisuje osoba lub osoby upoważnione do reprezentowania kontrolowanego podmiotu. W przypadku pełnomocnictwa do podpisania protokołu inspektor żąda jego przedstawienia.

Jak długo może trwać kontrola?

Termin trwania kontroli jest uzależniony m.in. od rodzaju kontroli, zakresu kontroli oraz wielkości kontrolowanego podmiotu. Termin jest ustalany przez Generalnego Inspektora, gdyż przepisy nie przewidują czasu trwania kontroli. Jednakże w odniesieniu do przedsiębiorców przepisy ustawy z dnia

2 lipca 2004 r. o swobodzie działalności gospodarczej (Dz.U. z 2007 r. Nr 155 poz. 1095) wskazują limity czasowe w obrębie danego roku kalendarzowego (art. 83 ust. 1).

Czy kontrola może być przeprowadzona w mieszkaniu prywatnym kontrolowanego podmiotu?

Czynności kontrolne mogą być wykonane w mieszkaniu prywatnym, jeżeli kontrolowany wskazał to mieszkanie jako siedzibę swojej firmy i miejsce prowadzenia działalności.

Czy inspektorzy posiadają poświadczenie bezpieczeństwa dostępu do informacji niejawnych?

Inspektorzy, zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. Nr 182, poz. 1228) posiadają poświadczenie bezpieczeństwa, upoważniające do dostępu do informacji niejawnych, stanowiących tajemnicę służbową, oznaczonych klauzulą „poufne".