Rozdział I

2

INSTRUKCJE DOTYCZĄCE OCHRONY DANYCH OSOBOWYCH W KANCELARII DORADZTWA PODATKOWEGO

- Jakie obowiązki spoczywają na doradcach podatkowych w związku z obowiązkiem ochrony danych osobowych?
- Jak powinna być sformułowana instrukcja przetwarzania danych osobowych w kancelarii doradztwa podatkowego?
- Jak zarządzać danymi osobowymi w kancelarii podatkowej?
- W jaki sposób chronić i zabezpieczać dane osobowe, aby uniknąć sankcji za naruszenie przepisów w tym zakresie?
- Jak stworzyć i zarządzać systemem informatycznym służącym do przetwarzania danych osobowych?

Instrukcja przetwarzania danych osobowych w Kancelarii Doradztwa Podatkowego[1]

ZAKRES OBOWIĄZYWANIA INSTRUKCJI

§ 1.

Instrukcja przeznaczona jest dla osób zatrudnionych w Kancelarii Doradztwa Podatkowego ..... w ..... (zwanej dalej Kancelarią Doradztwa Podatkowego) przy przetwarzaniu danych osobowych.

§ 2.

Ilekroć w instrukcji jest mowa o:

1) danych osobowych – należy przez to rozumieć wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
2) zbiorze danych – należy przez to rozumieć każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie;
3) przetwarzaniu danych – należy przez to rozumieć jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
4) usuwaniu danych – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
5) administratorze danych – należy przez to rozumieć Kancelarię Doradztwa Podatkowego – jako podmiot, do którego stosuje się ustawę o ochronie danych osobowych;

1 Stanowisko Krajowej Rady Doradców Podatkowych z dnia 7 maja 2008 r. w sprawie przyjęcia "Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz zarządzania polityką bezpieczeństwa" oraz "Instrukcji przetwarzania danych osobowych".

6) zgodzie osoby, której dane dotyczą – należy przez to rozumieć oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
7) systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
8) zabezpieczeniu danych w systemie informatycznym – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
9) administratorze bezpieczeństwa informacji – należy przez to rozumieć osobę odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;
10) administratorze systemu – należy przez to rozumieć osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi w Kancelarii Doradztwa Podatkowego.

ZAKRES PRZEDMIOTOWY INSTRUKCJI

§ 3.

Niniejsza instrukcja określa:
1) zasady postępowania przy przetwarzaniu danych osobowych;
2) prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych;
3) zasady rejestracji zbiorów danych osobowych;
4) zabezpieczenie zbiorów danych osobowych;
5) odpowiedzialność za naruszenie przepisów ustawy o ochronie danych osobowych i aktów wykonawczych.

§ 4.

1. Dane osobowe mogą być przetwarzane:
   1) w systemach informatycznych (mogą być nimi również pojedyncze komputery);
   2) w sposób tradycyjny – w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.
2. Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy, gdy spełniony jest co najmniej jeden z wymienionych poniżej warunków:
   1) osoba, której dane dotyczą, wyrazi zgodę na przetwarzanie danych (chyba, że chodzi o usunięcie dotyczących jej danych), zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, lecz musi wyraźnie doty-

czyć przetwarzania danych; wzór zgody osoby na przetwarzanie jej danych osobowych stanowi załącznik nr 1 do niniejszej instrukcji;
2) na przetwarzanie danych zezwalają przepisy prawa;
3) przetwarzanie danych jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia koniecznych działań przed zawarciem umowy;
4) przetwarzanie danych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
5) przetwarzanie danych jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratorów danych lub osób trzecich, którym są przekazywane te dane, a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą;
6) w innych przypadkach przewidzianych w przepisach prawa.

3. Jeżeli przetwarzanie danych jest niezbędne dla żywotnych interesów osoby, której dane dotyczą, a spełnienie warunków, o których mowa powyżej (w ust. 2 ppkt a), jest niemożliwe, administrator danych może przetwarzać dane bez zgody tej osoby, do czasu gdy uzyskanie tej zgody będzie możliwe.
4. Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazania, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydawanych w postępowaniu sądowym lub administracyjnym.
5. Przetwarzanie danych, o których mowa w ust. 3, jest dopuszczalne zgodnie z art. 27 ust. 2 ustawy o ochronie danych osobowych.

PRAWA OSÓB FIZYCZNYCH, KTÓRYCH DANE SĄ LUB MOGĄ BYĆ PRZETWARZANE W ZBIORACH DANYCH

§ 5.

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę:
   1) o istnieniu zbioru jej danych osobowych;
   2) o adresie swojej siedziby i pełnej nazwie;
   3) o celu zbierania danych, a w szczególności o znanych mu lub przewidywanych odbiorcach lub kategoriach odbiorców danych;
   4) o prawie wglądu do swoich danych oraz ich poprawiania;
   5) o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.
2. Obowiązek, o którym mowa w ust. 1 nie istnieje, jeżeli:
   1) ustawa zezwala na przetwarzanie danych bez ujawnienia faktycznego celu ich zbierania;
   2) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.

§ 6.

1. W przypadku uzyskania danych osobowych nie od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę bezpośrednio po utrwaleniu zebranych danych:
   1) o adresie swojej siedziby i pełnej nazwie;
   2) o celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;
   3) o źródle, z którego uzyskano dane;
   4) o prawie wglądu do swoich danych oraz ich poprawiania;
   5) o prawie żądania zaprzestania przetwarzania danych oraz o prawie sprzeciwu wobec przetwarzania danych.
2. Obowiązek, o którym mowa w ust. 1 nie istnieje, jeżeli:
   1) przepis prawa przewiduje lub dopuszcza zbieranie danych osobowych bez wiedzy osoby, której dane dotyczą;
   2) dane przewidziane do zebrania są ogólnie dostępne;
   3) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, a poinformowanie osób wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania;
   4) administrator danych nie przetwarza dalej zebranych danych po ich jednorazowym wykorzystaniu;
   5) dane są przetwarzane przez administratora danych na podstawie przepisów prawa;
   6) osoba, której dane dotyczą, posiada informacje, o których mowa w ust. 1.
3. Zobowiązuje się do prowadzenia ewidencji podmiotów, którym udostępniono dane osobowe.

§ 7.

1. Na administratorze danych ciąży obowiązek ochrony integralności i poprawności przetwarzanych informacji, szczególnie jest on obowiązany:
   1) przetwarzać je zgodnie z prawem;
   2) zbierać dane dla oznaczonych, zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami;
   3) gromadzić dane merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
   4) przechowywać je w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej, niż jest to niezbędne do osiągnięcia celu przetwarzania.
2. Przetwarzanie danych w celach innych niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, z zachowaniem przepisów art. 23 i 25 ustawy o ochronie danych osobowych.

§ 8.

1. Administrator danych przetwarzający dane w zbiorach, ma obowiązek udzielania informacji na wniosek osoby, której dane przetwarza i przestrzegania jej praw wynikających z ustawy, takich jak:
   1) prawo do informacji o:
      a) fakcie przetwarzania danych jej dotyczących,
      b) pełnym adresie siedziby i pełnej nazwie administratora danych,
      c) celu, zakresie i sposobie przetwarzania danych,
      d) dacie, od której dane zostały włączone do zbioru,
      e) treści danych,
      f) sposobie udostępniania danych oraz o odbiorcach lub kategorii odbiorców danych,
      g) źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy państwowej, zawodowej lub służbowej;
   2) prawo żądania uzupełnienia, uaktualnienia i sprostowania danych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane;
   3) prawo wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na szczególną sytuację, prawo to nie przysługuje, gdy administrator danych posiada zgodę osoby na wykorzystywanie danych, upoważnia go do tego przepis prawa lub gdy przetwarza dane w celu wykonania umowy;
   4) prawo wniesienia sprzeciwu wobec przetwarzania jej danych w celach marketingowych lub wobec przekazania jej danych osobowych innemu administratorowi danych;
   5) prawo wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej z naruszeniem art. 26a ust. 1 ustawy.
2. W przypadku wniesienia żądania, o którym mowa powyżej, administrator danych bez zbędnej zwłoki rozpatruje sprawę albo przekazuje ją wraz z uzasadnieniem swojego stanowiska Generalnemu Inspektorowi Ochrony Danych Osobowych, który wydaje stosowną decyzję.

§ 9.

1. Na wniosek osoby, której dane dotyczą, administrator danych jest obowiązany, w terminie 30 dni, poinformować o przysługujących jej prawach, a zwłaszcza wskazać w formie zrozumiałej odnośnie danych osobowych jej dotyczących:
   1) jakie dane osobowe zawiera zbiór;
   2) w jaki sposób zebrano dane;
   3) w jakim celu i zakresie dane są przetwarzane;
   4) w jakim zakresie oraz komu dane zostały udostępnione.

2. Informacji, o których mowa w ust. 1, udziela się na piśmie.

§ 10.

1. Administrator danych odmawia udostępnienia danych podmiotom i osobom, które nie są uprawnione do ich otrzymania na mocy przepisów prawa, jeżeli spowodowałoby to:
   1) ujawnienie wiadomości stanowiącej tajemnicę państwową lub zawodową;
   2) zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi, mienia lub bezpieczeństwa i porządku publicznego;
   3) zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa;
   4) istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.

ZASADY REJESTRACJI ZBIORÓW DANYCH OSOBOWYCH

§ 11.

1. Administrator danych – w sytuacjach przewidzianych w przepisach prawa – jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Danych Osobowych.
2. Administrator danych zwolniony jest z obowiązku, o którym mowa w ust. 1, w przypadkach określonych w art. 43 ust. 1 ustawy o ochronie danych osobowych.

ZABEZPIECZENIE ZBIORÓW DANYCH OSOBOWYCH

§ 12.

1. Administrator bezpieczeństwa informacji jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą lub utratą, uszkodzeniem lub zniszczeniem.
2. Szczegółowe wymogi w zakresie zastosowania środków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zawarte zostały w „Instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych ".

§ 13.

Zbiory danych osobowych podlegają ochronie i zabezpieczeniu:

1) po zakończeniu pracy dane osobowe winny być zabezpieczone w szafach zamykanych na klucz oraz pomieszczeniach, w sposób uniemożliwiający zapoznanie się z ich treścią osobom trzecim;

2) pojedyncze komputery zawierające dane osobowe powinny być zabezpieczone hasłem. Pracownicy zatrudnieni przy ich obsłudze nie mogą zezwalać na użytkowanie komputera osobom nieupoważnionym;
3) hasło umożliwiające dostęp do komputera definiuje administrator bezpieczeństwa informacji systemu;
4) przebywanie w pomieszczeniach osób nieupoważnionych jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych;
5) pomieszczenia powinny być zamykane na czas nieobecności w nich osób zatrudnionych;
6) monitory komputerów powinny być tak ustawione, aby uniemożliwić osobom postronnym wgląd do danych osobowych.

§ 14.

1. Pracownicy posiadający dostęp do danych osobowych winni złożyć oświadczenia o zachowaniu w tajemnicy danych osobowych oraz o zapoznaniu się z przepisami dotyczącymi ochrony danych.
2. Zobowiązuje się Administratora Bezpieczeństwa Informacji do pobierania oświadczeń, o których mowa w ust. 1, od nowo zatrudnionych pracowników.
3. Zakresy czynności osób zatrudnionych przy przetwarzaniu danych osobowych, w stopniu odpowiednim do zadań, powinny uwzględniać obowiązki z zakresu odpowiedzialności za bezpieczeństwo danych osobowych.
4. Oświadczenia, o których mowa w ust. 2, sporządza się w trzech egzemplarzach, z których po jednym egzemplarzu otrzymują:
   1) administrator danych;
   2) administrator bezpieczeństwa informacji;
   3) osoba składająca oświadczenie.

ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRZEPISÓW USTAWY O OCHRONIE DANYCH OSOBOWYCH

§ 16.

Zasady odpowiedzialności karnej za naruszenie obowiązków związanych z ochroną danych osobowych określa ustawa o ochronie danych osobowych.

§ 17.

Obowiązki i odpowiedzialność poszczególnych pracowników Kancelarii Doradztwa Podatkowego w zakresie ochrony i zabezpieczania danych osobowych powinien określać indywidualny zakres czynności tej osoby oraz upoważnienie do przetwarzania danych.

Opracowanie: Dominik Szczygieł

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz zarządzania polityką bezpieczeństwa w Kancelarii Doradztwa Podatkowego[1]

Stosownie do postanowień § 4 i 5 rozporządzenia 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 ze zm.), ustala się treść Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych polityki bezpieczeństwa, która znajdzie zastosowanie do danych osobowych przetwarzanych w systemie informatycznym oraz na innych nośnikach informacji w Kancelarii Doradztwa Podatkowego ..... w ....., zwanej dalej „KANCELARIĄ DORADZTWA PODATKOWEGO".

§ 1.

Na treść polityki bezpieczeństwa danych osobowych składają się:

1. wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe – załącznik nr 1;
2. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych – załącznik nr 2;
3. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi – załącznik nr 3;
4. sposób przepływu danych pomiędzy poszczególnymi systemami – załącznik nr 4;
5. określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych – załącznik nr 5.

1 Stanowisko Krajowej Rady Doradców Podatkowych z dnia 7 maja 2008 r. w sprawie przyjęcia "Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych oraz zarządzania polityką bezpieczeństwa" oraz "Instrukcji przetwarzania danych osobowych".