Dziennik Gazeta Prawna 27-10-2011

W jaki sposób pracodawca powinien przechowywać i chronić dane swoich pracowników

Przepisy ustawy o ochronie danych osobowych stanowią, że dane te powinny być zabezpieczone, a służące temu środki techniczne i organizacyjne są uzależnione od kategorii danych objętych ochroną

DR WOJCIECH RAFAŁ WIEWIÓROWSKI
generalny inspektor ochrony danych osobowych

Przetwarzanie danych osobowych w systemach teleinformatycznych reguluje osobne rozporządzenie wykonawcze do ustawy o ochronie danych osobowych. Jest to rozporządzenie ministra spraw wewnętrznych i administracji z 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.

Pracodawcy mają jednak problem z dostosowaniem się do jego wymagań, uznają je za przestarzałe i w efekcie nierzadko lekceważą jego regulacje. To prawda, że zawiera ono przepisy, które należałoby zastąpić nowymi. Takie działanie jest planowane na 2012 rok. Nie można jednak twierdzić, że jest ono całkowicie niedostosowane do dzisiejszych rozwiązań teleinformatycznych wykorzystywanych w Polsce.

Identyfikacja zbioru danych i dostęp do nich

Doświadczenia wskazują, że najwięcej problemów przysparza pracodawcy zidentyfikowanie zbiorów danych osobowych podlegających procedurze rejestracji oraz odpowiedź na pytanie, kiedy dochodzi do przetwarzania w zbiorze.

Najczęściej jako zbiory danych osobowych traktuje się wszystko, co fizycznie wygląda na zbiór – teczkę, skoroszyt, bazę danych znajdujących się w konkretnym komputerze czy na danym serwerze. Tymczasem każdy zestaw danych o charakterze osobowym, który da się ze sobą powiązać logicznie, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, stanowi zbiór danych osobowych.

Przyznanie określonym osobom prawa dostępu do danych osobowych stanowi w praktyce niemały problem.

W jednym ze szpitali upoważniono do tego wszystkie osoby sprzątające. Uznano, że ponieważ wchodzą do wszystkich pomieszczeń, to mogą zajrzeć do informacji o każdym pacjencie. Upoważniono je do dostępu do wszystkich danych, które znajdują się w szpitalu. Ten absurdalny przykład potwierdza częstą praktykę.

Pracodawcy, chcąc uniknąć problemu z ustaleniem, czy ktoś był upoważniony do dostępu do danych, na wszelki wypadek dają takie uprawnienia wielu osobom. Tymczasem prawidłowo wystawione (i prawidłowo zaewidencjonowane) upoważnienie do przetwarzania danych osobowych musi być związane z obowiązkami, które konkretny pracownik wykonuje. Przy czym zakres upoważnienia powinien być ściśle związany z zakresem obowiązków pracownika.

Uprawnienia do przetwarzania danych

Forma wydawania pracownikom upoważnień do przetwarzania danych osobowych i ich ewidencjonowania może być dowolna. Pracodawcy stosują różne metody – wystawiają je na papierze i ewidencjonują w papierowych zbiorach, ale też dokonują tego w systemie elektronicznym i w nim przechowują listę upoważnień. Mimo, że forma upoważnień może być dowolna, nie może być ono jednak udzielone ustnie, musi być jego ślad i taka ewidencja musi być obowiązkowo prowadzona.

Przy braku ewidencji nie można określić, kto, kiedy i w jaki sposób ma prawo przetwarzać dane. Nie jest przy tym ważne, czy obowiązek ewidencjonowania upoważnień będzie osobiście realizowany przez pracodawcę. Może to zadanie powierzyć np. konkretnemu pracownikowi lub wyspecjalizowanej jednostce w firmie zajmującej się kadrami. Może tym się zajmować administrator bezpieczeństwa informacji bądź jakikolwiek inny podmiot. To wewnętrzna decyzja pracodawcy. Musi być tylko jasne, kto taką ewidencję prowadzi.

Przechowywanie przez firmę zewnętrzną

Dane osobowe mogą być przechowywane przez firmę zewnętrzną.

Ilość danych osobowych w dużej firmie jest czasami tak ogromna, że pracodawcy wolą powierzyć ich przechowywanie wyspecjalizowanym podmiotom. To jednak wymaga sporządzenia umowy.

Artykuł 31 ustawy o ochronie danych osobowych przewiduje zawieranie tego typu umów. Zawarte w niej postanowienia, zobowiązania i prawa powinny gwarantować pracodawcy sprawowanie kontroli nad podmiotem, któremu powierzył przetwarzanie danych osobowych, o czym często się zapomina.

Tymczasem ustawa o ochronie danych osobowych wprost stanowi, że w przypadku zawarcia umowy powierzenia przetwarzania danych osobowych administrator danych wciąż jest odpowiedzialny za przestrzeganie jej przepisów. Skoro zatem pracodawca nadal jest odpowiedzialny za powierzone dane, to powinien zapewnić sobie możliwość kontroli nad podmiotem, któremu je przekazał.

Awaria systemu zawierającego dane

Każdy pracodawca musi się liczyć z tym, że może dojść do awarii systemu informatycznego, który jest wykorzystywany do przetwarzania danych osobowych. Dlatego zawczasu powinien przewidzieć procedury obowiązujące przy jej usuwaniu, w tym kwestie ochrony danych osobowych, w przypadku gdy naprawą systemu będą się zajmować osoby nieposiadające praw dostępu do danych lub podmiot zewnętrzny. W tym ostatnim przypadku ochronę danych i odpowiedzialność za nią należy uregulować w umowie zawieranej z firmą, która serwisuje sprzęt.

Odpowiedzialność karna

Administrator danych, którym jest również pracodawca, odpowiada za zgodne z prawem przetwarzanie danych osobowych.

Przepisy ustawy o ochronie danych osobowych w rozdziale 5 przewidują odpowiedzialność karną za naruszenie jej przepisów, niezależnie od tego, czy jest ono świadome, czy nieświadome. Kara grzywny, ograniczenia albo pozbawienia wolności grozi m.in. temu, kto:

- przetwarza w zbiorze dane osobowe, choć nie ma do tego prawa, lub w ogóle jest to niedopuszczalne,
- przechowuje w zbiorze dane osobowe niezgodnie z celem z celem jego utworzenia,
- narusza obowiązek odpowiedniego zabezpieczenia danych osobowych,
- udostępnia lub umożliwia dostęp do danych osobowych, mimo że jest zobowiązany do ich ochrony.

Odpowiedzialność karna za udostępnienie lub umożliwienie dostępu do danych osobom nieupoważnionym grozi także pracownikowi.

Ponadto trzeba pamiętać, że również przepisy kodeksu pracy zobowiązują pracownika do dbałości o dobro zakładu pracy oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Za wyrządzenie wspomnianej szkody kodeks pracy przewiduje odpowiedzialność służbową pracownika.

WZÓR

Kraków, dnia ..... 2011 r.

Generalny inspektor
ochrony danych osobowych
ul. Stawki 2
00-193 Warszawa

Administrator danych:
.....
.....

WNIOSEK
o nakazanie przywrócenia stanu zgodnego z prawem

W związku z naruszeniem przepisów o ochronie danych osobowych przez administratora danych polegającym na ..... na podstawie art. 18 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych wnoszę o nakazanie przywrócenia stanu zgodnego z prawem polegającego na:

■ uzupełnieniu, uaktualnieniu, sprostowaniu, udostępnieniu lub nieudostępnieniu danych osobowych.

UZASADNIENIE

.....
.....

Mając na uwadze powyższe, wnoszę jak na wstępie.

.....
(podpis)

Załączniki:
– odpis wniosku

Podstawa prawna

Art. 31 ustawy z 23 maja 1991 r. o związkach zawodowych (t.j. Dz.U. z 2001 r. nr 79, poz. 854 z późn. zm.) Rozporządzenie ministra spraw wewnętrznych i administracji z 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).