HAŚKO I SOLIŃSKA
SPÓŁKA PARTNERSKA ADWOKATÓW
ul. Nowa 2a lok. 15, 50-082 Wrocław
tel. (71) 330 55 55 fax (71) 345 51 11 e-mail: kancelaria@mhbs.pl

Wrocław, dnia 22.06.2015 r.

OPINIA	
przedmiot	**Praktyczne aspekty zmiany ustawy z dnia 29.08.1997 r. o ochronie danych osobowych** **– czy administrator danych, w tym placówka medyczna prowadząca działalność medyczną, musi powoływać administratora bezpieczeństwa informacji i zgłaszać go do GIODO,** **- jakie są inne obowiązki administratora danych związane z bezpieczeństwem danych osobowych wprowadzone na gruncie nowelizacji ustawy z dnia 29.08.1997 r. o ochronie danych osobowych oraz ewentualne konsekwencje grożące za ich niewykonanie?** **- Czy podmioty świadczące usługi lecznicze muszą zgłaszać zbiory danych swoich pacjentów do GIODO ? Czy do GIODO należy zgłaszać zbiory danych, które są prowadzone w wersji papierowej, jeśli zbiory te zawierają tzw. „dane wrażliwe" ?**
data	**22.06.2015 r.**

Podstawa prawna:

1. Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych z późn. zm. (Dz.U.1997.Nr 133 poz. 883), zwana również dalej : ustawą.

Stan faktyczny:

W związku z nowelizacją ustawy z dnia 29.08.1997 r. o ochronie danych osobowych powstały wątpliwości co do zakresu i sposobu realizacji obowiązków związanych z

przetwarzaniem zbiorów danych osobowych, jak również obowiązków związanych z funkcją administratora bezpieczeństwa informacji. Wątpliwości te dotyczą w szczególności:
- powoływania i zgłoszenia administratora bezpieczeństwa informacji do Generalnego Inspektora Ochrony Danych Osobowych (GIODO),
- terminu i sposobu przeprowadzenia audytu bezpieczeństwa informacji w celu sprawdzenia, które obszary ochrony danych należy poprawić,
- ewentualnych kar grożących pracodawcom na niewywiązanie się z nałożonych na nich na gruncie ustawy obowiązków,
- obowiązków dotyczących zgłaszania zbiorów danych osobowych do GIODO przez podmioty prowadzące działalność medyczną.

Stan prawny i ocena prawna:

Na wstępie zaznaczyć należy, iż podmiot będący administratorem danych już na gruncie poprzednio obowiązującego stanu prawnego (art. 40 ustawy) miał obowiązek zgłoszenia zbioru danych do rejestracji do GIODO. Obowiązek ten w zasadzie nie uległ zmianie. Wymieniony w art. 43 ustawy z dnia 29.08.1997 r. o ochronie danych osobowych katalog wyłączeń od obowiązku rejestracji zbioru danych został nawet minimalnie poszerzony (z korzyścią dla administratorów danych osobowych, którymi są na przykład podmioty prowadzące działalność medyczną). Katalog ten nie został bowiem w żadnym stopniu ograniczony, a wprowadzono nawet dodatkowe wyłączenie odnośnie zbiorów danych prowadzonych wyłącznie w postaci papierowej (od 01.01.2015 r. nie ma obowiązku zgłaszania ich do rejestracji do GIODO), chyba że zbiory te zawierają tzw. *„dane wrażliwe”* z art. 27. ust. 1 ustawy – wtedy ten obowiązek w dalszym ciągu istnieje.

Jest to rozwiązanie korzystne dla podmiotów prowadzących działalność leczniczą będących administratorami danych osobowych, **nie muszą oni bowiem po nowelizacji zgłaszać żadnych nowych zbiorów danych do rejestracji do GIODO,** zgłoszeniu podlegają wyłącznie te dane, których obowiązek zgłoszenia był już wcześniej nałożony na administratorów danych, a co więcej – jeśli zbiór danych prowadzony jest wyłącznie w formie papierowej i nie zawiera tzw. *„danych wrażliwych”*, **to nie ma już obowiązku zgłaszania takiego zbioru do GIODO.** Katalog wyłączeń od obowiązku rejestracji w

dalszym ciągu znajduje się w art. 43 ustawy o ochronie danych osobowych – jeśli dane są przetwarzane wyłącznie w celu wystawienia faktury lub rachunku bądź w związku z zatrudnieniem pracownika, czy to na umowę o pracę, czy cywilnoprawną, **to nie ma obowiązku rejestrowania takiego zbioru danych. Co więcej, podmioty udzielające świadczeń leczniczych nie mają obowiązku rejestracji zbioru danych osobowych swoich pacjentów u GIODO – takie zbiory objęte są wyłączeniem na podstawie art. 43 ust. 1 pkt. 5 ustawy, który stanowi o wyłączeniu z obowiązku rejestracji zbiorów danych dotyczących osób korzystających z usług medycznych administratora danych (czyli na przykład pacjentów placówek medycznych).**

Na gruncie przepisów ustawy z dnia 29.08.1997 r. o ochronie danych osobowych (z uwzględnieniem jej najnowszej nowelizacji) powołanie administratora bezpieczeństwa informacji jest **uprawnieniem** administratora danych osobowych, a nie jego obowiązkiem. Stanowi o tym wyraźnie treść art. 36a ustawy: „*administrator danych może powołać administratora bezpieczeństwa informacji”.* Administrator danych osobowych ma zgodnie z założeniami wprowadzonych przepisów przejąć większość wynikających z ustaw obowiązków podmiotów w zakresie administrowania danymi osobowymi. Jednakże, jeśli administrator bezpieczeństwa informacji nie zostanie powołany, obowiązki te w dalszym ciągu wykonuje administrator danych – czyli podmiot przetwarzający dane osobowe. Do tych obowiązków należy m.in.: przestrzeganie przepisów o ochronie danych osobowych czy prowadzenie i przetwarzanie ustawowo wymaganych rejestrów i baz danych. W sytuacji, gdy administrator bezpieczeństwa informacji nie zostanie powołany, pełną odpowiedzialność za przestrzeganie przepisów dotyczących ochrony danych osobowych ponosi administrator danych. W praktyce oznacza to, że placówka medyczna, jako administrator danych osobowych może dokonać wyboru, czy sama będzie odpowiedzialna za przetwarzanie danych zgodnie z normami i za zorganizowanie procesu przetwarzania danych, czy też zdecyduje się na powołanie administratora danych osobowych – w takiej sytuacji powierzy mu wykonywanie tych zadań. **Powołując administratora danych osobowych organizacja zdejmuje z siebie ciężar ustawowych obowiązków – przenosi je wtedy na administratora bezpieczeństwa informacji.** Jeśli podmiot zdecyduje się na powołanie administratora bezpieczeństwa informacji ma on w dalszym ciągu obowiązek zgłoszenia do GIODO jedynie rejestru danych zawierających dane wrażliwe – a więc dane wymienione w art. 27 ust. 1

ustawy (czyli: dane 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 skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym). **W tym miejscu zaznaczyć należy, że pomimo uznania przez ustawodawcę danych o stanie zdrowia za dane wrażliwe, to podmioty świadczące działalność leczniczą nie mają obowiązku rejestracji danych swoich pacjentów u GIODO – dla takich zbiorów danych ustawodawca przewidział bowiem zwolnienie z obowiązku rejestracji, o czym już wcześniej wspomniano.**

W sytuacji, gdy administrator danych (przykładowo placówka medyczna) zdecyduje się jednak na powołanie administratora bezpieczeństwa informacji, placówka medyczna ma obowiązek (zgodnie z brzmieniem przepisu art. 46b ust. 1 ustawy) w terminie 30 dni zgłosić ten fakt do GIODO (taki sam 30 dniowy termin obowiązuje w wypadku odwołania administratora bezpieczeństwa informacji przez administratora danych). Szczegółowe informacje dotyczące danych, które należy zgłosić do GIODO wymienione są w art. 46b ustawy – są to dane dotyczące głównie osoby, która ma sprawować funkcję administratora bezpieczeństwa informacji. W wypadku zmiany tych danych (na przykład zmianę adresu do korespondencji administratora bezpieczeństwa informacji), zmianę tę placówka medyczna powinna zgłosić w terminie 14 dni od momentu zaistnienia zmiany.

Administrator bezpieczeństwa informacji z założenia ma wykonywać swoją funkcję w sposób niezależny – istotnym zagadnieniem może okazać się wprowadzony na gruncie nowelizacji przepis art. 19 b ustawy – GIODO będzie mógł zwrócić się do wpisanego do rejestru administratora bezpieczeństwa informacji o dokonanie zgodności przetwarzania danych osobowych zgodnie z przepisami, wskazując zakres i termin sprawdzenia. W sytuacji, gdy administrator bezpieczeństwa informacji zostanie powołany, podmiot, który go zatrudnia nie będzie miał wpływu na sposób dokonania przez niego weryfikacji.

Na koniec zaznaczyć należy, iż nie uległy zmianie przepisy karne zawarte w ustawie z dnia 29.08.1997 r. o ochronie danych osobowych.

Wnioski:

W związku z nowelizacją ustawy z dnia 29.08.1997 r. **nie powstał obowiązek powoływania administratora bezpieczeństwa informacji. Jest to jedynie uprawnienie administratora danych.** Należy jednak pamiętać, że w wypadku niepowołania administratora bezpieczeństwa informacji, za spoczywające na nim obowiązki odpowiedzialny będzie w dalszym ciągu administrator danych (z wyłączeniem obowiązku administratora bezpieczeństwa informacji polegającym na sporządzeniu sprawozdania dla administratora danych). W tym zakresie nowelizacja nie ma wpływu na dotychczasowe obowiązki administratora danych, gdyż przed wejściem w życie nowelizacji był on również odpowiedzialny za zgodną z prawem, a w szczególności z przepisami ustawy o ochronie danych osobowych, organizację procesu przetwarzania danych osobowych.

Podstawową różnica, jaka nasuwa się po analizie przepisów ustawy polega na tym, **że w wypadku powołania administratora bezpieczeństwa informacji nie trzeba zgłaszać do GIODO zbiorów danych zwykłych** (a więc zbiorów danych, które nie są danymi wrażliwymi w rozumieniu art. 27 ust. 1 ustawy, ani których zgłoszenie nie jest wyłączone na podstawie art. 43 ustawy) **przetwarzanych w systemach informatycznych. Powołanie administratora bezpieczeństwa informacji nie wpłynie natomiast na zgłaszanie danych wrażliwych - te dane trzeba zgłaszać niezależnie od tego, czy podmiot zdecyduje się na powołanie administratora bezpieczeństwa informacji czy też nie, chyba że obowiązek ich zgłoszenia został przez ustawodawcę wyłączony (tak jest w przypadku zbiorów danych pacjentów placówek medycznych – nie trzeba ich zgłaszać).**

Tak naprawdę decyzja o powołaniu administratora bezpieczeństwa informacji zależy od uznania administratora danych, czy jest w stanie samodzielnie zadbać o właściwe przetwarzanie danych i wypełniać obowiązki z tym związane.

Na koniec stwierdzić należy jeszcze, że nie ma obowiązku rejestracji zbioru danych pracowników przetwarzanych w związku z zatrudnieniem ich u administratorów danych (nie ma obowiązków zgłaszania do GIODO zbiorów danych osób zatrudnionych w placówkach medycznych), czy też świadczeniem im usług na podstawie umów cywilnoprawnych oraz przetwarzanych wyłącznie w celu wystawienia faktury czy rachunku (art. 43 pkt. 4 i 7 ustawy nie uległy zmianie).

Nowelizacja nie wprowadziła również żadnych nowych przepisów karnych, nie zawiera również informacji odnośnie przeprowadzenia audytu bezpieczeństwa informacji w celu sprawdzenia, które obszary ochrony danych zarządzanych przez administratora danych należy poprawić. Żaden z przepisów znowelizowanej ustawy nie nakłada bowiem na administratora danych (czyli na przykład na placówkę medyczną) takiego obowiązku.