

Poradnik e-Commerce Polska. Zmiany dotyczące ustawy o ochronie danych osobowych

Szanowni Członkowie i Partnerzy Izby Gospodarki Elektronicznej,

W związku z faktem, iż działalność e-commerce niejednokrotnie wiąże się z przetwarzaniem danych osobowych klientów, czy kontrahentów sklepów internetowych, pragniemy zwrócić Państwa uwagę na najważniejsze zmiany ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (zwanej dalej: Ustawą), które weszły w życie z dniem 1 stycznia 2015 r., a także na nowe rozporządzenia wykonawcze, które weszły w życie w dniu 30 maja 2015 r.

Część obowiązków, realizowanych do tej pory przez Generalnego Inspektora Ochrony Danych Osobowych (zwanego dalej: GIODO) przeniesiona została na administratorów danych osobowych (zwanymy dalej: ADO) i w konsekwencji, na powołanych przez nich administratorów bezpieczeństwa informacji (zwanymy dalej: ABI). Ponadto, nowelizacja Ustawy wprowadziła istotne uproszczenia w zakresie rejestracji zbiorów danych osobowych.

I Zwolnienie z obowiązku rejestracji

Znowelizowana Ustawa zawiera m.in. szerszy niż dotychczasowy katalog zwolnień z obowiązku rejestracji zbiorów danych osobowych. Od 1 stycznia 2015 r. wprowadzono kolejne zwolnienie obejmujące zbiory prowadzone bez wykorzystania systemów informatycznych, w których nie są przetwarzane dane wrażliwe.

Ponadto, obowiązkowi rejestracji zbiorów danych osobowych, z wyjątkiem zbiorów zawierających dane wrażliwe, nie podlega ADO, który powołał ABI i zgłosił go GIODO do rejestracji. Oznacza to, że co do zasady ADO przetwarzający dane nie mające charakteru danych wrażliwych, który wyznaczył w swojej organizacji ABI oraz wypełnił odpowiednie zgłoszenie i przesłał je do biura GIODO, w ogóle nie będzie musiał zgłaszać zbiorów danych do GIODO.

II Nowe obowiązki ABI

ADO może powołać ABI, do którego zadań będzie należało, w szczególności:

- 1) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla ADO,
- 2) nadzorowanie opracowania i aktualizowania polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, jak również przestrzegania zasad określonych w tych dokumentach,
- 3) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- 4) prowadzenie jawnego rejestru zbiorów danych przetwarzanych przez ADO, z wyjątkiem zbiorów zwolnionych z obowiązku rejestracji.

Ponadto, ADO może powierzyć ABI wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa powyżej.

W przypadku niepowołania ABI zadania wskazane powyżej, z wyłączeniem obowiązku sporządzania sprawozdania, wykonuje ADO.

Rozporządzenia wykonawcze, które zostały wydane w związku z nowelizacją Ustawy określają szczegółowy tryb i sposób realizacji zadań oraz sposób prowadzenia rejestru

zbiorów danych przez ABI.

III Zgłoszenie powołania/odwołania ABI do rejestru

ADO jest obowiązany zgłosić do rejestracji GIODO powołanie i odwołanie ABI w terminie 30 dni od dnia jego powołania lub odwołania.

ABI powinien spełniać następujące warunki:

- 1) mieć pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych;
- 2) posiadać odpowiednią wiedzę w zakresie ochrony danych osobowych;
- 3) być niekaranym za umyślne przestępstwo.

Nadto ABI musi podlegać bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej ADO, zaś ADO obowiązany jest zapewnić środki i organizacyjną odrębność ABI niezbędne do niezależnego wykonywania przez niego zadań.

Zgłoszenie powołania i odwołania ABI GIODO powinno nastąpić na formularzach, których wzory określa rozporządzenie wykonawcze do nowelizacji Ustawy. W rozporządzeniu tym określono nadto szczegółowy zakres danych, które winny być zawarte w zgłoszeniu powołania i odwołania ABI.

ADO jest obowiązany zgłosić GIODO zmianę informacji objętych zgłoszeniem, o którym mowa powyżej, w terminie 14 dni od dnia zmiany. Do zgłaszania zmian stosuje się odpowiednio przepisy o zgłoszeniu powołania ABI.

Jeśli wolą ADO jest, aby dotychczasowy ABI pełnił tę funkcję po zmianie przepisów Ustawy, ABI musi spełniać warunki opisane powyżej. W takim przypadku ABI wyznaczony przed dniem 1 stycznia 2015 r. powinien zostać zgłoszony do rejestracji GIODO do dnia 30 czerwca 2015 r. Jeżeli ADO zaniecha zgłoszenia dotychczasowego ABI do rejestracji, po 30 czerwca 2015 r. przestaje on pełnić tę funkcję, a zadania ABI (z wyłączeniem obowiązku sporządzania sprawozdania) zobowiązany jest wykonywać ADO, który ponosi pełną odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych.

IV Nowy rejestr GIODO

W związku z wprowadzeniem nowego rodzaju zgłoszeń, powstał nowy ogólnokrajowy jawny rejestr ABI, który prowadzony jest przez GIODO. W rejestrze ABI ujawnione są dane ADO oraz informacje o ABI.

Zgodnie z nowymi przepisami Ustawy, GIODO z urzędu wydawał będzie decyzję o wykreśleniu danego ABI z rejestru, jeśli nie będzie spełniał on wymogów określonych w Ustawie (tj. posiadania pełnej zdolności do czynności prawnych i korzystania z pełni praw publicznych, posiadania odpowiedniej wiedzy w zakresie ochrony danych osobowych, niekaralności za przestępstwo umyślne oraz podlegania bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej ADO) lub też jeśli ABI nie będzie realizował zadań powierzonych mu zgodnie z Ustawą, a także w sytuacji gdy ADO nie powiadomi GIODO o odwołaniu ABI.

V Nowe zasady przekazywania danych poza Unię Europejską

W myśl znowelizowanych przepisów Ustawy przekazanie danych osobowych do państwa trzeciego, które nie zapewnia na swoim terytorium odpowiedniego poziomu ochrony danych osobowych (do państw takich zaliczane są w szczególności USA) nie wymaga już uzyskania zgody GIODO, jeżeli ADO zapewni odpowiednie zabezpieczenia w zakresie

ochrony prywatności oraz praw i wolności osoby, której dane dotyczą, przez:

- 1) standardowe klauzule umowne ochrony danych osobowych, zatwierdzone przez Komisję Europejską zgodnie z art. 26 ust. 4 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, lub
- 2) prawnie wiążące reguły lub polityki ochrony danych osobowych (zwane dalej: wiążącymi regułami korporacyjnymi), które zostały zatwierdzone przez GIODO.

W celu odpowiedniej oceny przedłożonych do zatwierdzenia reguł, GIODO może przeprowadzać konsultacje z właściwymi organami ds. ochrony danych z państw należących do Europejskiego Obszaru Gospodarczego. Jeżeli wiążące reguły korporacyjne były przedmiotem rozstrzygnięcia organu ochrony danych osobowych innego państwa należącego do Europejskiego Obszaru Gospodarczego – GIODO może uwzględnić to rozstrzygnięcie.

VI Nowe kompetencje GIODO

W Ustawie dodano nowy przepis przyznający GIODO prawo zwrócenia się do ABI, wpisanego do rejestru, o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i opracowania w tym zakresie sprawozdania dla GIODO.

Oczywiście, niezależnie od dokonania przez ABI sprawdzenia, GIODO będzie mógł przeprowadzić u danego ADO kontrolę.

Komentarz eksperta e-Izby – radcy prawnego Olgierda Porębskiego:

Nowe przepisy przewidują opcjonalność powoływania w firmie ABI, jednocześnie znacznie rozszerzając zakres obowiązków ABI oraz akcentując konieczność posiadania odpowiedniej wiedzy przez osobę sprawującą tę funkcję. Powierzenie obowiązków ABI osobie nieprzygotowanej, co miało dotychczas często miejsce, będzie obecnie wiązało się z większym ryzykiem zarówno dla firmy, jak i dla tej osoby.

Można przypuszczać, że powołanie ABI, któremu GIODO może polecać czynności sprawdzające, będzie w praktyce powodowało, iż zamiast prowadzić kontrole, GIODO znacznie częściej będzie ograniczał się do uzyskiwania sprawozdań od ABI.

Jeśli ABI nie zostanie powołany, wszystkie jego obowiązki (oprócz sporządzania sprawozdań) obciążają szefa firmy.