

Jak radzić sobie z danymi osobowymi

Przygotowując wyjazdy incentive, agencje gromadzą dużą ilość danych osobowych swoich klientów. Ich właściwa ochrona oraz przetwarzanie mogą okazać się sporym wyzwaniem.

Pierwszym problemem jest już samo określenie, czym są właściwie dane osobowe. Ustawa mówi, że mogą to być jakiegokolwiek dane, które pozwalają zidentyfikować konkretną osobę, o ile nie wymaga to nadmiernych kosztów, czasu lub działań. Granica jest więc dość płynna i może być różnie interpretowana. Sytuację komplikuje dodatkowo podział danych osobowych na tzw. dane zwyczajne oraz dane wrażliwe. Pierwsze to spotykane najczęściej informacje, takie jak imię, nazwisko, adres czy numer telefonu. Do drugich zaliczają się m.in. pochodzenie rasowe, poglądy polityczne, przekonania religijne, dane o stanie zdrowia czy nałogach. Biura incentive, z racji specyfiki wykonywanych zadań, bardzo często spotykają się również z wrażliwymi danymi, które bywają przydatne w organizacji wyjazdu.

Agencja administratorem

Największe obowiązki dotyczące właściwego zarządzania danymi osobowymi spoczywają na ich administratorze. Jest nim podmiot, który decyduje, w jaki sposób, przy użyciu jakich środków i w jakim celu będą przetwarzane te dane. Teoretycznie, jeśli agencja dostaje od swojego klienta, czyli zleceniodawcy wyjazdu, listę osób, które wezmą w nim udział, nie decyduje o celu wykorzystania danych, a tym samym nie staje się jeszcze ich administratorem. Jeżeli jednak w jakikolwiek sposób agencja wykorzysta otrzymane dane na własny użytek, automatycznie staje się ich administratorem, razem ze wszystkimi obowiązkami wynikającymi z tego tytułu. Dotyczy to zarówno danych osobowych spisanych w formie papierowej, jak i tych umieszczonych w systemach informatycznych. W praktyce takie przetwarzanie danych osobowych zdarza się bardzo często, chociażby w sytuacji, gdy agencja przechowuje otrzymane dane po zakończeniu wyjazdu, dla swoich własnych celów.

Konieczna rejestracja

Na administratorze danych osobowych, którym, jak wynika z praktyki, bardzo często staje się agencja incentive, spoczywa wiele obowiązków, zarówno w relacjach z GODO (Generalny Inspektor Ochrony Danych Osobowych), jak i z osobami, których te dane dotyczą. Po pierwsze należy zarejestrować taki zbiór danych osobowych w GODO. Rejestracja bazy danych odbywa się raz, jej późniejsze aktualizacje i uzupełnienia nie wymagają już kolejnych zgłoszeń. Co istotne, dane zwyczajne można przetwarzać od razu, od chwili zgłoszenia zbioru, natomiast da-

ne wrażliwe mogą zostać przetworzone w jakikolwiek sposób dopiero od chwili rejestracji zbioru w GODO. Agencja musi posiadać odpowiednią podstawę do przetwarzania danych, to znaczy, że musi być jej to niezbędne do wykonania umowy, czyli w tym przypadku do organizacji wyjazdu incentive. Kolejną ważną rzeczą jest wypełnienie obowiązku informacyjnego wobec osób, których dane znajdują się w bazie. Osoby te muszą zostać poinformowane przez kogo ich dane będą wykorzystywane, w jakim celu oraz muszą mieć świadomość o prawie dostępu do danych oraz prawie ich poprawiania. W tym celu należy przedstawić do podpisu (w formie papierowej) lub odznaczenia (w formie elektronicznej) każdej z osób znajdujących się w bazie stosowną klauzulę o ochronie danych osobowych. Także w przypadku przekazywania danych za pośrednictwem platformy rejestracyjnej, uruchomionej przez firmę incentive, wskazane jest zamieszczenie na końcu formularza checkboxu z klauzulą dotyczącą wyrażenia zgody na przetwarzanie danych osobowych. Nie istnieje bowiem domniemana zgoda na ich przetwarzanie.

Zabezpieczanie danych

Po spełnieniu wszystkich wymogów formalnych przetwarzane przez agencję dane osobowe muszą być stosownie zabezpieczone. Polskie przepisy bardzo restrykcyjnie podchodzą do tego zagadnienia. Dane osobowe w formie papierowej powinny być przechowywane w szafie wyposażonej w zamek patentowy. Szafa powinna znajdować się w pomieszczeniu, do którego dostęp mają tylko osoby upoważnione. W praktyce jest to warunek bardzo trudny do realizacji. Jeżeli segregatory z danymi osobowymi znajdują się w pomieszczeniu, do którego pod nieobecność osób upoważnionych wstęp mogą mieć jakiegokolwiek osoby trzecie (na przykład klienci lub serwis sprzątający), to w świetle przepisów prawa warunek ten nie jest dopełniony i inspektor GODO może wyciągnąć konsekwencje wobec takiego biura. Pojawiają się także dodatkowe wymogi dotyczące odpowiedniego zabezpieczenia pomieszczenia, w którym znajdują się dane. Wskazane jest zainstalowanie na przykład systemu przeciwpożarowego oraz monitoringu. Wymogi tego typu wydają się paradoksalne i mogą być uciążliwe, szczególnie dla małych biur, których po prostu nie stać na tego typu infrastrukturę. Nie mniejsze obostrzenia dotyczą danych przechowywanych w systemach informatycznych, na komputerach stacjo-

narych lub laptopach, szczególnie, jeżeli są one podłączone do internetu. Komputery takie muszą zostać przykładowo zabezpieczone przed nieautoryzowanym uruchomieniem (choćby za pomocą hasła BIOS blokującego włączenie komputera przez osoby nieupoważnione), także systemy operacyjne komputera, w którym przetwarzane są dane osobowe powinny być chronione za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika i hasła, które należy okresowo zmieniać. W przypadku przesyłania danych za pośrednictwem e-maili, wiadomości takie bezwzględnie powinny zostać zaszyfrowane.

Co z podwykonawcami?

Otrzymując zbiór danych osobowych uczestników wyjazdu incentive od klienta agencji, winna ona podpisać z nim umowę powierzenia przetwarzania danych osobowych. Dokument ten określa przede wszystkim, jakie dane są powierzone do przetwarzania, w jakim celu oraz jaki ma być stosowany przez agencję standard zabezpieczeń. W przypadku powierzenia przez agencję danych osobowych osób, biorących udział w wyjeździe, podwykonawcom, którzy będą realizować zlecenie dla klienta we współpracy z agencją powinno się sporządzić odpowiednią pisemną umowę dalszego powierzenia przetwarzania danych osobowych temu podwykonawcy. Podwykonawca również powinien posiadać poziom zabezpieczeń danych osobowych przynajmniej na takim samym poziomie, jak administrator. W praktyce trudno jest to sprawdzić, szczególnie w przypadku partnerów w egzotycznych i odległych krajach, do których często odbywają się wyjazdy incentive. Warto pamiętać, że umowa powierzenia danych osobowych nie jest jednak konieczna w przypadku przesyłania tychże danych do ambasad (na przykład w celu wyrobienia wizy), gdyż te placówki mogą mieć do nich swobodny dostęp, co wynika z oddzielnych regulacji prawnych. Podobnie rzecz wygląda w przypadku hoteli, jeżeli dane osobowe podawane są w celach meldunkowych. Przy rezerwacjach lotniczych przyjęto zasadę, że w przypadku

podania przewoźnikowi jedynie imion i nazwisk osób, którym zostaną wystawione bilety (co ma miejsce w większości przypadków) również nie trzeba uzyskiwać dodatkowych zezwoleń. Przy okazji organizacji wyjazdów incentive transfer danych osobowych klientów za granicę jest czymś naturalnym, z czym agencja spotyka się bardzo często. Pełna swoboda przesyłania danych osobowych, czyli na takich samych zasadach, jak w Polsce możliwa jest jedynie do krajów Unii Europejskiej oraz Norwegii, Lichtensteinu i na Islandię. Poza tym obszarem możliwe jest przesyłanie danych do państw, w których standard ich ochrony jest co najmniej taki, jak w Polsce (stosowna lista została przygotowana przez Komisję Europejską) oraz za zgodą zainteresowanego lub gdy przekazanie danych jest konieczne do wykonania umowy. W praktyce, w przypadku przesyłania danych do państw trzecich, które nie znajdują się na żadnej z list, najlepiej uzyskać zgodę osób, których dane mają zostać przekazane. Pozwoli to uniknąć nieporozumień, agencja nie będzie również musiała udowodnić, że przekazanie danych było niezbędne do wykonania umowy, czyli w tym przypadku do realizacji podróży incentive.

Poważne konsekwencje

Niejednokrotnie trudno w pełny sposób zabezpieczyć dane osobowe. Przepisy w tym względzie są bardzo restrykcyjne. W praktyce, w przypadku wykrycia niezbyt rażących nieprawidłowości, inspektorzy GODO nie podejmują od razu kroków mających na celu ukarania winowajcy, ale starają się edukować w tym zakresie i wprowadzać stosowne poprawki. Warto jednak zadbać o zarejestrowanie bazy danych oraz jej odpowiednie zabezpieczenie, aby nie dostała się w ręce osób nieuprawnionych, tym bardziej, że za przetwarzanie danych osobowych bez podstawy prawnej może grozić odpowiedzialność karna i cywilna. Konieczne jest także dopełnienie obowiązku informacyjnego oraz zniszczenie wszystkich dokumentów zawierających dane osobowe po ustaniu ich przydatności.

*Michał Kalarus, pomoc ekspercka:
Piotr Niezgodka, Kochański Zięba
Rapala i Partnerzy Sp. j.*

DOSSIER

Gdzie można bezpiecznie przesyłać dane osobowe

Lista państw, które zostały uznane przez Komisję Europejską za zapewniające odpowiednią ochronę danych osobowych (stwierdzenie to jest jednoznaczne z tym, że kraje te zapewniają takie same gwarancje ochrony, jakie obowiązują w Polsce): **Argentyna, Australia, Guernsey, Izrael, Jersey, Kanada, USA, Szwajcaria, Wyspa Man, Wyspy Owcze.** Oprócz tego wszystkie kraje UE oraz **Norwegia, Lichtenstein i Islandia.**