

Kłopotliwe dane osobowe

Praktycznie każdy sklep internetowy musi we właściwy sposób **postępować z informacjami** pozyskiwanymi od swoich klientów. Można w tym celu zatrudnić ABI albo zarejestrować się w GODO

Patrycja Otto
patrycja.otto@infor.pl

Aż 35 proc. właścicieli e-sklepów błędnie uważa, że nie musi rejestrować zbioru danych osobowych w GODO – wynika z najnowszego badania przeprowadzonego wśród 8 tys. internetowych placówek przez serwis SafeBuy.pl i Sklepy24.pl. W błąd może wprowadzać ich też informacja, zawarta na stronie zarządzanej przez UOKiK, zgodnie z którą „jeżeli korzystamy danych osobowych wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej, to zawierającego je zbioru nie musimy zgłaszać do rejestracji GODO”.

Co i po co gromadzimy

Niemal 100 proc. sklepów internetowych nie zbiera danych osobowych wyłącznie w tych celach. Każdy, kto więc choć raz kupował online wie, że są one pozyskiwane, by zawrzeć i zrealizować umowę sprzedaży, w tym w szczególności w celu realizacji prawa do odstąpienia od umowy przez konsumentów, ale przede wszystkim w celu dostarczenia przesyłki – komentuje Piotr Jarosz, prezes zarządu serwisu SafeBuy.pl i współautor kodeksu dobrych praktyk eCommerce Fair Play. – W takim przypadku nie znam przepisu, który zwalniałby administratora danych osobowych z obowiązku rejestracji zbioru danych w GODO, dlatego nie rozumiem celu informacji zamieszczonych na portalu Ezakupy.UOKiK.gov.pl. Moim

zdaniem takie informacje są szkodliwe, gdyż mogą wprowadzać w błąd – dodaje.

Według GODO materiał na stronie UOKiK jest poprawny, choć zawiera jedynie przykładowe sytuacje, w których trzeba bądź nie zgłaszać zbioru danych do rejestracji. Dodaje, że otrzymał do konsultacji od UOKiK rozszerzoną wersję notatki.

Od początku tego roku, w związku z nowelizacją ustawy o ochronie danych osobowych, zmieniły się zasady rejestracji zbiorów danych osobowych. Zgodnie z nowymi przepisami e-sklepy, ale też

inni przedsiębiorcy prowadzący działalność, nie muszą rejestrować zbiorów danych u generalnego inspektora ochrony danych osobowych, jeśli powołają administratora bezpieczeństwa informacji (ABI) i zgłoszą go do rejestracji GODO. Innym wyjątkiem są zbiory danych, które nie są prowadzone z wykorzystaniem systemów informatycznych. Nie ma to jednak zastosowania w przypadku sklepów internetowych.

ABI zabezpieczy

– O powołaniu ABI decyduje administrator danych. Jeśli uzna, że jest w stanie samodzielnie zadbać o ich prawidłowe przetwarzanie i zaprowadzić nad tym procesem, to nie ma takiego obowiązku – informuje Andrzej Lewiński, zastępca generalnego inspektora ochrony danych osobowych. Dodaje jednak, że to rozwiązanie przydatne. – W społeczeństwie rośnie świadomość potrzeby ochrony danych. Świadczy o tym chociażby liczba skarg, jakie do nas w tym zakresie wpływają. Wiele z nich jest uzasadnionych. Rośnie też świadomość samych administratorów danych, choć nadal pozostawia wiele do życzenia. Wielu ciągle nie zna podstawowych obowiązków, jakie nakładają na nich przepisy. Dlatego warto skorzystać z pomocy osób

mających wiedzę w tym zakresie, czyli ABI – dodaje Andrzej Lewiński.

Osoby te odpowiadają nie tylko za kwestie techniczne związane z prawidłowym zabezpieczeniem systemów informatycznych, szyfrowaniem danych, ale też dbają o to, by nie były one narażone na ataki cyberprzestępców.

Administratora bezpieczeństwa informacji można wyłonić spośród pracowników. Trzeba tylko pamiętać, że taka osoba powinna mieć odpowiednie przygotowanie i wiedzę z zakresu przepisów o ochronie danych osobowych. Można ją nabyć, biorąc udział w szkoleniu. Na rynku jest obecnie wiele firm, które oferują kształcenie w tym kierunku.

– Kurs trwa cztery dni i składa się z trzech części. Na koniec otrzymuje się certyfikat administratora bezpieczeństwa danych – tłumaczy Anna Felczak z firmy Kerberos Ochrona Informacji. Za szkolenie trzeba zapłacić od 2 do 3 tys. zł.

Ekspert podpowiada, że na tym stanowisku najlepiej sprawdzi się osoba z wiedzą prawniczą i informatyczną. – Osoba taka nie może być też karana za przestępstwo z winy umyślnej oraz musi móc korzystać w pełni z praw publicznych – wyjaśnia Andrzej Lewiński.

Alternatywne rozwiązanie to outsourcing tego rodzaju usług. Na rynku jest wiele firm, które oferują pomoc w zakresie ochrony danych osobowych. Koszt zarówno jednego, jak i drugiego rozwiązania waha się od kilkuset złotych do kilku tysięcy. Wiele zależy bowiem od wielkości firmy oraz zakresu obowiązków firmy lub pracownika.

W razie powołania ABI firma ponosi też koszty wynikające z prowadzenia jawnego rejestru zbioru danych. Trzeba bowiem stworzyć platformę internetową do przechowywania danych. W przypadku mniejszych firm wystarczy, że będą one gromadzone w postaci pliku HTML. Zatem tylko duże firmy, mające rozbudowane zbiory, mogą potrzebować dodatkowego narzędzia. Pracodawcy poniosą też koszty przygotowania przez ABI dla administratora danych wewnętrznych sprawozdań oraz wykonywanych przez niego czynności na zlecenie GODO.

Zgłoszenie i nie tylko

Jeśli e-sklep nie powoła ABI, to zgodnie z nowymi przepisami musi ustalić, czy jest zobowiązany dokonać rejestracji zbioru danych osobowych do GODO, czy może istnieją przesłanki zwalniające go z obowiązku. Odbywa się to poprzez przesłanie do urzędu należytego wypełnionego formularza

zgłoszeniowego. Trzeba odpowiedzieć w sumie na 18 pytań.

Abi to jednak zrobić prawidłowo, trzeba mieć merytoryczną wiedzę np. na temat poziomu zabezpieczeń danych osobowych w firmie, tego, czy ich zbiór jest rozproszony, czy nierozproszony, czyli czy jest zgromadzony na serwerze, czy w segregatorze w wersji papierowej.

– Przygotowaliśmy prosty w obsłudze generator wniosku zgłoszenia zbioru danych osobowych. Wystarczy w nim odpowiedzieć na dwa pytania – czy e-sklep wybrał ABI oraz komu powierzył przetwarzanie danych osobowych. Jest on jednak dostępny tylko dla uczestników naszego programu eCommerce Fair Play, którzy wypełniając wniosek, udzielają nam wszelkich innych informacji, dzięki którym jesteśmy w stanie uzupełnić pozostałą część zgłoszenia do GODO – tłumaczy Piotr Jarosz.

Ekspert zauważa, że w przypadku małych firm zdecydowanie tańszym rozwiązaniem będzie zgłoszenie zbioru danych do GODO niż powołanie ABI. Zwłaszcza że powiadomienie oraz późniejsza aktualizacja informacji są nieodpłatne.

Według nich dobrze jest jednak wynająć ABI na 2-3 miesiące, bo rola administratora danych nie kończy się na zgłoszeniu rejestru do GODO. Jego obowiązkiem jest też opracowanie i wdrożenie polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym czy prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych. Zakres polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym szczegółowo opisuje rozporządzenie ministra spraw wewnętrznych. Dlatego ich opracowanie warto zlecić firmie świadczącej takie usługi.

– Koszt takiego opracowania jest uzależniony od wielkości organizacji, której dotyczy, oraz od złożoności procesów związanych z ochroną danych osobowych, jednak w przypadku małego lub średniego sklepu internetowego nie powinien być wyższy niż kilkaset złotych – wylicza Piotr Jarosz.

Od ABI można natomiast wszystkiego się nauczyć. A warto zdobyć potrzebną wiedzę, bo GODO ma w planach zwiększenie liczby kontroli.

Rośnie branża, rosną bazy danych

Co sądzą sprzedawcy:

CZY TRZEBA ZGŁASZAĆ ZBIÓR DANYCH OSOBOWYCH KONSUMENTÓW DO GODO?

65%
TAK, ZAWSZE MA TAKI OBOWIĄZEK

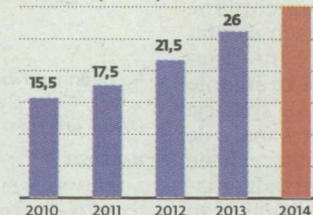
22%
NIE, DANE TE SĄ ZBIERANE W CELU REALIZACJI UMOWY

13%
NIE, DANE TE SĄ ZBIERANE W CELU WYSTAWIENIA FAKTURY

Badanie przeprowadzone na 8 tys. sklepów w dniach 9-11 grudnia 2014 r.

POLSKI RYNEK E-COMMERCE

Wartość (mld zł)



Liczba sklepów internetowych (tys.)



Źródło: Sklepy24.pl, Internet Standard

Na razie nie karano surowo

Niezarejestrowanie zbioru danych osobowych wiąże się z odpowiedzialnością karną z art. 53 ustawy o ochronie danych osobowych, czyli z karą grzywny, karą ograniczenia wolności albo pozbawienia wolności do roku. Karze podlega administrator danych zatrudniony w danej firmie. Jak dotąd zostały nałożone zaledwie dwie kary grzywny. Administratorzy danych powinni mieć jednak świadomość, że już w tym roku może zostać uchwalone unijne rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Jego projekt jest już w zasadzie gotowy, a prace nad dopracowaniem jego ostatecznej wersji idą bardzo sprawnie. Rozporządzenie zmieni i ujednolici reguły ochrony danych osobowych w całej Unii Europejskiej. I, co bardzo istotne, przewiduje ono surowe kary finansowe za naruszenie przepisów – będą liczone od obrotu firmy, czyli może to być nawet 100 mln euro. Kara będzie nakładana nie jak dotąd na administratora danych, ale na firmę, w której jest zatrudniony. Jeżeli nowe przepisy wejdą one w życie, to automatycznie będą stosowane także w Polsce.