Warszawa, 25.10.2023 r.

Dane osobowe w sklepie stacjonarnym – jak je chronić?

Ochrona danych osobowych w sklepie stacjonarnym jest istotnym aspektem, szczególnie w kontekście przestrzegania przepisów ogólnego rozporządzenia o ochronie danych osobowych (RODO). Zdecydowana większość poradników skupia się na zabezpieczeniu danych osobowych w środowisku cyfrowym co powoduje, że zapominamy, że dużą część danych przetwarzamy w formie tradycyjnej.

Oto kilka kroków, które pomogą Ci chronić dane osobowe w Twoim sklepie:

1. Na dobry początek, co oczywiste, zapoznaj się z przepisami RODO, aby dokładnie zrozumieć swoje obowiązki i odpowiedzialności w zakresie ochrony danych osobowych. Kluczowe będą tu przede wszystkim te przepisy, które dotyczą przesłanek dających uprawnienia do gromadzenia danych, obowiązki informacyjne, a także uprawnienia jakie przysługują Twoim klientom – konsumentom (ale też osobom fizycznym prowadzącym działalność gospodarczą).
2. Zidentyfikuj, jakie dane osobowe zbierasz i przetwarzasz w swoim sklepie. To mogą być informacje o klientach (np. reklamacje, zgłoszenia dotyczące rękojmi, skargi), pracownikach (np. grafiki pracy, dane kontaktowe, rankingi pracownicze), kandydatach do pracy (przede wszystkim składane bezpośrednio do sklepu CV), dostawcach (np. listy osób uprawnionych do odbioru pieniędzy z kasy) itp.
3. Wyznacz osobę odpowiedzialną za nadzór nad prawidłową ochroną danych osobowych. To może być zarówno właściciel sklepu, jak i pracownik, który ma odpowiednie kompetencje. Jeśli Twój sklep funkcjonuje w ramach większej sieci, to istnieje duże prawdopodobieństwo, że został wyznaczony inspektor ochrony danych (IOD) w centrali – być może istnieją jakieś wytyczne, które zostały przez niego przygotowane, materiały szkoleniowe, itp. Na pewno warto (a nawet trzeba) być z IOD w stałym kontakcie.
4. Ogranicz ilość zbieranych danych osobowych do absolutnie niezbędnego minimum w celu realizacji określonych celów.
5. Przetwarzaj dane osobowe wyłącznie wtedy, gdy posiadasz do tego odpowiednią podstawę prawną np. gromadzenie danych wynika z przepisu prawa (gwarancja, rękojmia, faktury), zawartej umowy (reklamacje) albo zgody na przetwarzanie danych (np. jeśli masz program lojalnościowy). To jest istotne zwłaszcza w przypadku marketingu lub zbierania danych w innych celach niż konieczne do transakcji handlowych – w takich przypadkach najprawdopodobniej będziesz musiał posiadać stosowną zgodę.
6. Informuj klientów oraz pozostałe osoby, których dane przetwarzasz o tym, jakie dane osobowe są zbierane i w jakim celu. Udostępnij im także informacje na temat ich praw związanych z danymi osobowymi. Dość powszechną praktyką w sklepach jest umieszczenie stosownego „standu" na ladzie zawierającego wszystkie powyższe informacje (tzw. klauzula informacyjna).
7. Ogranicz dostęp do danych osobowych tylko do osób, które potrzebują ich do wykonania swoich obowiązków służbowych.
8. Zabezpiecz fizycznie dokumenty oraz urządzenia, na których przechowywane są dane osobowe. Wyposaż pomieszczenia w zamykane szafy, sejfy i zamki na drzwiach. Upewnij się, że tylko upoważnieni pracownicy mają dostęp do tych pomieszczeń.
9. Jeśli używasz urządzeń elektronicznych do przetwarzania danych osobowych (np. komputery kasowe), zabezpiecz je hasłami i korzystaj z oprogramowania antywirusowego oraz zapory sieciowej.
10. Przechowuj dane osobowe tylko przez okres niezbędny do realizacji celów, na jakie zostały zebrane, a następnie usuń je zgodnie z obowiązującymi przepisami dotyczącymi konkretnych kategorii danych. I ponownie – jeśli działasz w ramach większej sieci sklepów, w tym zakresie na pewno trzeba skontaktować się z IOD. Jeśli nie masz IOD, czeka Cię nieco więcej pracy, bo musisz poszukać w przepisach prawa jak długo poszczególne dane mogą być przechowywane, a w niektórych przypadkach samodzielnie wyznaczyć rozsądny okres ich retencji.

11. Przeszkol swoich pracowników w zakresie ochrony danych osobowych, aby zrozumieli ich znaczenie i wiedzieli, jakie informacje są uważane za dane osobowe i jak prawidłowo się z nimi obchodzić. W przypadku bycia częścią większej sieci, tego typu szkolenia są bardzo często realizowane przez IOD.
12. Opracuj procedury postępowania z danymi osobowymi np. w przypadku incydentów, zgłoszenia się kandydata do pracy, przechowywania dokumentacji pracowniczej, zabezpieczenia komputera na stanowisku pracy, itp. Tu także, w przypadku bycia częścią większej sieci, tego typu procedury opracowywane są przez IOD.
13. Regularnie przeprowadzaj audyty wewnętrzne w celu oceny zgodności z przepisami RODO i identyfikacji obszarów wymagających poprawy. Taki audyt może przeprowadzić IOD, ale można też skorzystać z pomocy zewnętrznej firmy, która świadczy usługi doradcze w zakresie audytu ochrony danych osobowych.

Zapewnienie ochrony danych osobowych w sklepie stacjonarnym jest ważne nie tylko ze względów prawnych, ale także dla budowania zaufania klientów i utrzymania dobrej reputacji firmy. Dbanie o prywatność klientów jest kluczowym elementem.

Maria Lothamer – ekspert ds. ochrony danych, Wiceprezes Zarządu w iSecure Sp. z o.o.