Zarządzanie programem lojalnościowym w zgodzie z RODO/GDPR po 25 maja 2018 roku

Na co powinni zwrócić uwagę organizatorzy programów lojalnościowych w kontekście nowych przepisów RODO?

Rozporządzenie nr 2016/679 (tzw. RODO/GDPR) w dniu 25 maja 2018 roku zacznie obowiązywać w całej Unii Europejskiej. Wprowadza szereg nowych i zmienionych wymagań dla wszystkich organizacji, które gromadzą i przechowują dane osobowe np. klientów. Również firmy z sektora FMCG muszą na czas dostosować swoje działania, procedury i dokumentację.

Ocena ryzyka od etapu projektowania programu lojalnościowego

RODO wymaga, aby już na etapie projektowania procesów, np. programu lojalnościowego, uwzględniono ocenę ryzyka i jego potencjalnych skutków dla ochrony danych oraz mechanizmów bezpieczeństwa i prywatności. Zadanie to nie jest łatwe, szczególnie gdy w realizację programu lojalnościowego zaangażowanych jest wiele osób z organizacji oraz zewnętrznych partnerów i podwykonawców.

Skutkiem naruszenia zasad RODO może być zarówno odejście klientów i utrata reputacji firmy, jak i sankcje finansowe. Z tych powodów nawet najlepiej zaprojektowane i wdrożone zabezpieczenia procesów przetwarzania danych w programach lojalnościowych powinny podlegać regularnej, obiektywnej ocenie skuteczności stosowanych procedur, narzędzi i kultury organizacyjnej. Aby uzyskać obiektywną weryfikację zgodności podejmowanych działań z wymaganiami RODO organizatorzy programów lojalnościowych coraz częściej zlecają przeprowadzenie specjalistycznego audytu niezależnym ekspertom.

Legalność przetwarzania danych osobowych

Kluczowym aspektem jest legalność przetwarzania danych uczestników programu lojalnościowego. Należy zweryfikować podstawę prawną, a w szczególności zgody na przetwarzanie danych udzielone przez osoby zgłoszone do programu. Audytorzy ocenią m.in. konstrukcję zgody, sprawdzając, czy została pozyskana w sposób dobrowolny, konkretny, świadomy i jednoznaczny. Niezbędne jest aktywne zaangażowanie uczestnika w wyrażenie zgody, np. powinien zaznaczyć wcześniej puste pole formularza, własnoręcznie podpisać formularz itd.

Zgodnie z wprowadzoną przez RODO tzw. zasadą rozliczalności organizator programu lojalnościowego musi umieć wykazać, że osoba, której dane dotyczą, wyraziła taką zgodę. Istotne jest też udowodnienie, że każdy uczestnik programu może łatwo wycofać zgodę, że jego dane będą przetwarzane dokładnie tyle czasu, ile jest konieczne dla potrzeb programu oraz że wszystkie stosowane praktyki są zgodne z regulaminem.

Ocena ryzyk związanych z przetwarzaniem danych osobowych

Poziom akceptacji ryzyka powinien być uzgodniony z kierownictwem oraz uwzględniać dobre praktyki i specyfikę branży. Do procesów przetwarzania danych należy włączyć monitorowanie ryzyka lub jego ponowną

ocenę w przypadku zmian w procesach (np. zmiana regulaminu programu, nowy dostawca itp.). Administrator musi umieć uzasadnić, dlaczego zastosował określone środki bezpieczeństwa przetwarzana danych.

Ważne jest wdrożenie w firmie procesów zarządzania ryzykiem pod kątem zasady „*privacy by design*", polegającej na uwzględnianiu ochrony danych osobowych już w fazie projektowania programu, oraz zasady „*privacy by default*" - domyślnej ochrony danych. Audytorzy sprawdzą też, jak są monitorowane ryzyka w procesie zarządzania zmianą.

Zgoda na przetwarzanie danych przed przystąpieniem do programu

W każdym przypadku zgoda musi zostać uzyskana, **zanim** uczestnik będzie korzystał z programu lojalnościowego. Uzyskanie zgody musi dawać **rzeczywisty wybór** przystąpienia do programu. Nie może być domyślnie aktywne, ograniczone do wybranych operacji przetwarzania danych marketingowych, a wycofanie lub odmowa jej udzielenia nie może prowadzić do negatywnych konsekwencji. Ponadto musi się odnosić w jasny i czytelny sposób osobno do każdego z celów przetwarzania danych.

Aby zapewnić spełnienie warunku uzyskania świadomej zgody, istotne jest spełnienie obowiązku informacyjnego. Uczestnika programu należy poinformować o tożsamości administratora danych, o celu oraz o tym, jakie dane będą przetwarzane. Administrator powinien również poinformować uczestnika m.in. o przysługującym mu prawie do wycofania zgody, o tym, czy stosuje profilowanie, czy dane będą przekazywane do krajów spoza UE (np. gdy dane z formularza online przechowywane są na serwerze w USA).

Gromadzenie danych osobowych w placówkach handlowych

W wielu placówkach handlowych oferowanie potencjalnym uczestnikom udziału w programach lojalnościowych jest jednym z zadań doradcy klienta. Aby zapewnić bezpieczne przetwarzanie danych w tym obszarze niezbędne jest wdrożenie adekwatnych do ryzyk zabezpieczeń organizacyjnych i technicznych. Audytor sprawdzi m.in. świadomość personelu w zakresie obowiązywania wewnętrznych regulacji oraz ich zastosowanie w praktyce, np. przechowywanie dokumentów papierowych w szafach pod kluczem, używanie niszczarek dokumentów, ochrony antywirusowej komputerów itd.

Usuwanie i niszczenie danych osobowych

Jeśli wycofano zgodę lub upłynął czas na przetwarzanie danych w związku z określonym celem, wszystkie operacje przetwarzania danych muszą zostać zaprzestane. W świetle RODO w takiej sytuacji dane powinny zostać usunięte, łącznie z kopią bezpieczeństwa, lub zanonimizowane przez administratora. Audytor sprawdzi, w jaki sposób klient może wycofać zgodę, oraz jak informacja o cofnięciu zgody jest procesowana w organizacji.

Uczestnictwo dzieci w programie lojalnościowym

Przetwarzanie danych dzieci jest zgodne z prawem wyłącznie w przypadku, gdy zgoda została udzielona lub zatwierdzona przez osobę sprawującą władzę rodzicielską lub opiekę nad dzieckiem, oraz wyłącznie w zakresie wyrażonej zgody. Sposób weryfikacji wieku uczestnika programu lojalnościowego powinien być adekwatny do oceny ryzyk, z uwzględnieniem dostępnych technologii. Może to być np. rozmowa telefoniczna z opiekunem dziecka.

Odpowiedzialność za ochronę danych osobowych

Odpowiedzialność za ochronę danych spoczywa zarówno na kierownictwie, jak i na pracownikach liniowych organizatora programu lojalnościowego. Niezbędne jest zapewnienie wsparcia i zasobów ze strony menedżerów (np. budżet na ochronę danych) oraz świadomość i zaangażowanie personelu. Oprócz formalnych procedur, ważne są takie elementy, jak: czyste biurko, polityka haseł, zasady zgłaszania incydentów itp.

Ochrona danych w programie organizowanym we współpracy z zewnętrznymi podmiotami

Organizator programu lojalnościowego może udostępnić dane osobowe fundatorowi nagród, powierzyć je w celu wsparcia obsługi np. zewnętrznej firmie informatycznej lub współorganizatorowi programu. RODO nakłada obowiązek wyboru dostawców w sposób gwarantujący ochronę danych i praw osób fizycznych. W pierwszym przypadku należy sprawdzić, czy uzyskano legalnie zgodę na takie udostępnienie oraz czy dopełniono obowiązku informacyjnego np. w regulaminie. W drugim przypadku mamy do czynienia z przekazaniem danych osobowych uczestników programu tzw. *procesorowi*. Audytorzy zweryfikują zgodność stosowania zapisów art. 28 rozporządzenia, tj. formę umowy powierzenia, zasady podpowierzania danych w łańcuchu dostawców oraz zasady nadzoru nad dostawcą przez organizatora.

Jeżeli program lojalnościowy organizowany jest wspólnie przez 2 lub więcej firm, mamy do czynienia z nową instytucją *współadministratora*. Weryfikacji w tym przypadku zostaną poddane przede wszystkim zasady odpowiedzialności stron. Eksperci zbadają świadomość i stosowanie w praktyce przyjętych zasad ochrony danych osobowych wśród personelu partnerów i dostawców programu lojalnościowego.

Dokumentacja wymagana w zakresie ochrony danych osobowych

Przepisy RODO zmieniają dotychczasowe ujednolicone podejście do tworzenia dokumentów w zakresie danych osobowych. Obecna ustawa o ochronie danych osobowych oraz rozporządzenie MSWiA dość precyzyjnie wskazują zakres i strukturę dokumentacji. Wg nowego podejścia punktem wyjścia jest analiza ryzyk oraz ocena skutków dla ochrony danych, prowadzona najlepiej w formie udokumentowanej informacji, która ma zapewnić możliwość wykazania rozliczalności administratora danych. Za wyjątkiem kilku wskazanych wprost dokumentów, jak np. rejestr czynności przetwarzania, czy zasady obsługi naruszeń bezpieczeństwa, **pozostałe zabezpieczenia organizacyjne** (procedury, instrukcje, kultura organizacyjna) i zabezpieczenia techniczne (teleinformatyczne, fizyczne, środowiskowe) muszą kompensować zidentyfikowane ryzyka w konkretnej organizacji.

Naruszenie ochrony danych osobowych

Intencją twórców rozporządzenia było minimalizowanie negatywnych skutków majątkowych i niemajątkowych osób, których dotyczy naruszenie ochrony danych. Aby je zapewnić należy ustalić w organizacji proces identyfikowania takich sytuacji na wszystkich szczeblach zarządzania i upewnić się, że został on skutecznie wdrożony. Istotne jest, czy pracownicy mają możliwość dogodnego zgłoszenia przypadków naruszeń, czy organizacja ma procedury gromadzenia dowodów z naruszeń i ich oceny oraz czy ustalono proces zgłaszania i informowania zainteresowanych stron.

Audyt ochrony danych osobowych

Zlecając zewnętrzny audyt, dobrze jest zapewnić jego realizację w dwóch fazach. Najpierw klient dokonuje wstępnej samooceny w oparciu o specjalnie przygotowane narzędzie online. Celem tego etapu jest analiza gotowości do audytu z perspektywy audytora oraz przygotowanie się do audytu z perspektywy klienta. Audyt na miejscu, przeprowadzany przez niezależnych ekspertów, uwzględnia ocenę procesów przetwarzania danych osobowych w powiązaniu ze spełnieniem obowiązków prawnych oraz skuteczność zastosowanych mechanizmów bezpieczeństwa.

Rozporządzenie RODO/GDPR zacznie obowiązywać 25 maja br. W tym samym dniu ma wejść w życie znowelizowana ustawa o ochronie danych osobowych oraz unijne przepisy dotyczące ochrony danych w komunikacji elektronicznej. Przedsiębiorstwa czekają poważne zmiany, których celem jest zapewnienie bezpieczeństwa i przejrzystości zasad przetwarzania danych osobowych. Organizatorzy programów lojalnościowych, którzy spełnią wytyczne krajowych i europejskich regulacji prawnych, dodatkowo wzmocnią swój pozytywny wizerunek.

Piotr Ubych

Menedżer Produktu ds. Ochrony Danych

Grupa DEKRA w Polsce

www.dekra.pl