RAPORT Z AUDYTU U ŚWIĘTEGO MIKOŁAJA

Minęło ponad 2,5 roku od kiedy stosujemy RODO. W grudniu 2018 po raz pierwszy zadaliśmy sobie pytanie, czy RODO obowiązuje także Świętego Mikołaja? Dla wątpiących: obowiązuje :)

W tym roku poszliśmy krok dalej i sprawdziliśmy, jak Święty Mikołaj radzi sobie z zapewnianiem zgodności z RODO. Zadaliśmy Mikołajowi szereg pytań dotyczących wdrożenia RODO w jego działalności. Na tej podstawie powstał raport.

Niech będzie on dla Państwa świątecznym prezentem i wywoła chwilę uśmiechu w tym pełnym wyzwań roku 2020.

PODMIOTY ZAANGAŻOWANE

Inspektor Ochrony Danych

Święty Mikołaj (dalej jako: Administrator lub Mikołaj) jeszcze w czerwcu 2018 r. wyznaczył inspektora ochrony danych (IOD). Decyzją Mikołaja funkcję tę objęła jego żona. Jak ustalono, administrator w żaden sposób nie opublikował jednak danych kontaktowych IOD. Zarekomendowano ich publikację, tak by dzieci wiedziały jak kontaktować się z Mikołajem w sprawach dotyczących ich danych osobowych.

Zwrócono także uwagę na konflikt interesów IOD. Okazało się bowiem, że żona Mikołaja piastuje u Administratora również inne funkcje, w tym funkcję ASI (administratora systemów informatycznych) oraz Głównej Księgowej. Żona Mikołaja utrzymuje jednak, że jest osobą niekonfliktową i nie widzi problemu w opisanej sytuacji.

Osoby upoważnione

Wszystkie elfy zaangażowane w proces przetwarzania danych osobowych dzieci otrzymały od Administratora stosowne upoważnienia oraz zobowiązały się do zachowania informacji w tajemnicy. Istnieje jednak poważny problem – emerytowanym elfom nikt nie odbiera upoważnień do przetwarzania danych. Mikołaj obiecał wykonać przegląd upoważnień zaraz po świętach.

Upoważnienia otrzymał również personel techniczny Mikołaja, w tym renifery. Zwrócono uwagę na tę niewłaściwą praktykę, a personel techniczny ma zostać zobowiązany jedynie do podpisania (odciskiem kopyta) oświadczeń o poufności.

DOKUMENTOWANIE PROCESÓW PRZETWARZANIA DANYCH OSOBOWYCH

Dokumentacja RODO

Dokumentacja RODO została wdrożona (z wyjątkiem, o którym mowa poniżej). Niektóre elfy odmówiły zapoznania się z jej treścią, argumentując „A po co mi to". Z tym elfami przeprowadzono rozmowy dyscyplinujące (w szczególności przypomniano im podstawowe obowiązki pracownicze).

U Administratora nie jest prowadzony rejestr czynności przetwarzania. Jako uzasadnienie takiego stanu rzeczy wskazano art. 30 ust. 5 RODO (zdaniem Administratora jest mniej niż 250 osób zatrudnionych, a przetwarzanie nie stwarza dużego ryzyka). Powrót do tematu zaplanowano na po Nowym Roku.

Naruszenia

Jeden z elfów (menedżer ds. misiów pluszowych) zapisał login i hasło do systemu IT Mikołaja na karteczce i zgubił ją. Znalazło ją dziecko JK (inicjały zmieniono), zalogowało się do systemu i przeniosło się z listy niegrzecznych dzieci na listę grzecznych dzieci. Naruszenie zostało wykryte i zgłoszone do fińskiego organu nadzorczego z opóźnieniem. Urząd nie potwierdza, by otrzymał takie zgłoszenie (ale i nie zaprzecza).

UMOWY POWIERZENIA

Podczas przeglądu zawartych przez Administratora umów powierzenia, odnaleziono kilkaset porozumień o powierzeniu przetwarzania danych zawartych z rodzicami dzieci. Mikołaj argumentował, że taką praktykę rekomendowano na internetowych forach IOD. Jak podkreślał podczas audytu, rodzice pomagają mu w kompletowaniu prezentów, co – jego zdaniem – czyni ich podmiotami przetwarzającymi dane dzieci w imieniu Mikołaja.

Wyjaśniono Mikołajowi, że rodzice pełnią tu rolę opiekunów prawnych podmiotów danych, wobec czego Mikołaj zobowiązał się anulować umowy powierzenia z rodzicami najpóźniej w Sylwestra.

EOG

Wobec unieważnienia Tarczy Prywatności przez Trybunał Sprawiedliwości UE istnieją poważne obawy związane z dostarczeniem paczek do dzieci w USA. Rada Konsultacyjna przy Świętym Mikołaju (dane osobowe członków rady zostały niestety utajnione z uwagi na RODO) zarekomendowała nawet zaprzestanie wysyłania paczek amerykańskich dzieci do pomocników Mikołaja w USA i przekazanie całej operacji Santa Clausowi.

Swoje pytania w sprawie transferu danych na terytorium USA Mikołaj zgłosił do EROD i fińskiego organu nadzorczego. Na chwilę obecną Mikołaj nie otrzymał jednak jeszcze stanowisk tych organów.

BEZPIECZEŃSTWO

Etykietowanie prezentów

Mikołaj używa narzędzia do automatycznego etykietowania prezentów. Baza danych jest backupowana (zgodnie z zasadą 3-2-1) przez podmiot zewnętrzny – ten sam, który dokonuje serwisowania narzędzia. Ustalono, że podmiot ten odmówił podpisania umowy powierzenia, twierdząc, że nie przetwarza danych osobowych. ASI nie odniósł się do tematu. Zarekomendowano rozważenie zmiany firmy świadczącej usługę serwisu i kopii zapasowych.

Kamery monitoringu

Po stwierdzeniu licznych incydentów podjadania cukierków ze służbowej choinki w warsztacie zainstalowano monitoring wizyjny. Ponieważ obraz nie jest rejestrowany, nie dochodzi do przetwarzania danych osobowych i tym samym nie ma konieczności stosowania RODO. Notabene liczba podkradanych słodyczy po instalacji kamer spadła o 50%.

ŚWIADOMOŚĆ PERSONELU

W trakcie audytu ustalono, że w zeszłym roku nie przeprowadzono szkoleń uzupełniających nt. zasad przetwarzania danych osobowych w fabryce Mikołaja. Były planowane na czerwiec 2020 r., ale odwołano je ze względu na pandemię.

Szkolenia online nie były możliwe do przeprowadzenia z uwagi na problemy elfów z obsługą programu do pracy zdalnej SANTA TEAMS.

INFORMOWANIE O PROCESACH

Ustalono, że Administrator nie realizuje wobec dzieci obowiązków informacyjnych zgodnie z art. 13 RODO. IOD argumentował, że wobec Mikołaja znajduje zastosowanie wyłączenie z art. 13 ust. 4 RODO, bowiem dzieci wierzą w Mikołaja i tym samym wiedzą, kto jest administratorem ich danych osobowych.

Zarekomendowano Mikołajowi warstwową realizację obowiązku informacyjnego poprzez nadrukowywanie kodów QR na paczkach, które trafiają do dzieci oraz publikację obowiązku informacyjnego na stronie internetowej Mikołaja.

INNE

W jednej z szafek (w gabinecie lidera ds. lalek) znaleziono listy prezentów sprzed 25 lat. Zgodnie z obowiązującą u Administratora instrukcją kancelaryjną takie dokumenty powinny być usuwane po 12 miesiącach. Nakazano bezpieczne usunięcie danych przez: 1) spalenie znalezionych dokumentów w kominku żony Mikołaja, 2) komisyjne rozsianie popiołów na cztery wiatry, 3) sporządzenie protokołu zniszczenia.

WESOŁYCH ŚWIĄT!

Zespół JAMANO