Warszawa, 07.12.2022r

Szkolenia RODO a świadomość pracowników w zakresie ochrony danych osobowych

„To jeszcze *szkolenie z RODO*…"

Szkolenie z zakresu ochrony danych osobowych jest obecnie jednym z obowiązkowych szkoleń dla nowozatrudnionych osób. Zdecydowanie jednak powinien to być *jeden z*, a nie *jedyny* moment, w którym pracownicy stykają się z tematyką ochrony danych osobowych. W idealnym świecie pracownicy na co dzień pracujący z danymi osobowymi stosują odpowiednie zabezpieczenia, są uważni, skupieni i nie pozwalają sobie na błędy. Niemniej jednak błąd ludzki stanowi ponad połowę przyczyn występowania naruszeń ochrony danych osobowych (za: sprawozdanie Prezesa Urzędu Ochrony Danych Osobowych za 2021 r.)

Dlaczego szkolenie z ochrony danych osobowych jest tak dobrym, a tak niedocenionym narzędziem?

Przede wszystkim jest to narzędzie bardzo elastyczne. Szkolenie może być przeprowadzone w formach: stacjonarnej, webinaru oraz e-learningowej. Może być ogólnym wstępem do ochrony danych osobowych dla wszystkich pracowników na każdym stanowisku, jak również dopasowane do branży, organizacji i grupy stanowisk. Może być skupione na procedurach organizacyjnych, przepisach sektorowych lub wewnętrznych zdarzeniach.

Niezależnie od wybranej formy szkolenia, jeden aspekt pozostaje niezmienny: rozliczalność, tj. udokumentowanie obecności osób uczestniczących w szkoleniu. Tradycyjne listy obecności cieszą się nieustającym powodzeniem, w ostatnich latach również w formie elektronicznego wykazu osób uczestniczących w spotkaniu on-line. Czy tradycyjne listy skanować i przechowywać na dysku? Czy listy elektroniczne drukować i przechowywać w segregatorze, w oryginale, podpisane przez osobę prowadzącą szkolenie? Każde z tych rozwiązań będzie dobre. Na uwagę zasługuje forma e-learningu, która daje możliwość wygenerowania raportu potwierdzenia obecności oraz ugruntowania wiedzy pracowników, poprzez rozwiązanie testu wiedzy. Analogicznie do szkolenia BHP, pozytywne rozwiązanie testu może warunkować dopuszczenie pracownika do pracy. Niektórzy z Inspektorów Ochrony Danych (i nie tylko) fantazjują o wymogu uzależnienia ukończenia testu z pozytywnym wynikiem z możliwością zalogowania się do domeny komputera służbowego.

Dlaczego piszę, że szkolenie z RODO jest niedocenianym narzędziem? Głównie dlatego, że wydaje się pracownikom zbędne i nieciekawe. Jednak praktyka zawodowa pokazuje, iż pracownicy często nie wiedzą, czy w organizacji są przyjęte procedury związane z ochroną danych osobowych ani gdzie je znaleźć. Mimo, że poza szkoleniem *face to face*, prawdopodobnie otrzymali procedurę w e-mailu, to nie zapoznali się z jej treścią. Pracownicy nie wiedzą na przykład, jakie zdarzenia podlegają zgłoszeniu do Inspektora Ochrony Danych (lub osoby wyznaczonej przez Administratora, w przypadku braku konieczności powołania IOD). Czy w firmie jest taka osoba? Na jaki adres mailowy zgłosić incydent i jakie informacje przekazać? Czy obowiązują jakieś terminy w odpowiedzi na wniosek osoby o udostępnienie jej kopii danych? Jakie są wytyczne do usuwania danych – z poczty służbowej, z systemów informatycznych? Kto i za co odpowiada? Po dobrze zorganizowanym szkoleniu pracownicy i współpracownicy Administratora powinni przynajmniej wiedzieć, że wytyczne w tym zakresie obowiązują i gdzie mogą je znaleźć.

Kiedy zorganizować *szkolenie z RODO*?

Wspomniałam o elemencie onboardingu pracownika. Kolejną okazją do przeprowadzenia szkolenia jest przyjęcie lub zmiana przepisów wewnętrznych lub zewnętrznych. Zwłaszcza, gdy aktualizacja obejmuje tę część pracy, za którą jest odpowiedzialny Administrator, a w praktyce właściciel biznesowy danej czynności przetwarzania. Jeżeli zmiana dotyczy np. dokumentacji, którą przygotowuje lub wypełnia właściciel biznesowy, warto poświęcić czas na omówienie wymogów względem „produktu końcowego".

Zatrzymam się na chwilę przy materiałach wspierających, dotyczących szkolenia związanego z przyjęciem lub zmianą procedur. Moim ulubionym materiałem dla pracowników po przeprowadzeniu szkolenia jest tzw. roadmap-a, dokument roboczo przeze mnie nazywany „rozkładem jazdy po procedurach". Samodzielne wyodrębnienie najważniejszych informacji z danej procedury przez pracowników i prawidłowe przypisanie poszczególnych zadań jako swoją odpowiedzialność oraz późniejsze pamiętanie o nich po miesiącach czy latach zatrudnienia, może przysporzyć problem. Wystarczy jednak krótki wyciąg z procedur, ze wskazaniem odpowiedzialności poszczególnych grup stanowisk. Tego oczekujemy od skutecznego szkolenia: przyswojenia wiedzy przez pracowników i współpracowników o funkcjonujących w organizacji dokumentach, o tym, kiedy je stosujemy i o tym, jaka wynika z nich odpowiedzialność.

Nieoczywistym momentem na przeprowadzenie szkolenia z ochrony danych osobowych jest zmiana struktury organizacji. Tego rodzaju zmiany niosą za sobą konieczność weryfikacji rejestrów czynności i kategorii czynności przetwarzania, przypisania czynności lub umów do właścicieli biznesowych, a także weryfikacji, w czyim zakresie odpowiedzialności pozostaje kontynuacja trwających analiz. Stronami uczącymi się w tym kontekście będzie zarówno IOD jak i właściciele biznesowi poszczególnych czynności przetwarzania.

Szkolenie po stwierdzonym naruszeniu

Szkolenie może być również następstwem zgłoszenia naruszenia do Prezesa UODO, będącym środkiem zaradczym występowaniu kolejnych naruszeń. Wyodrębniam to szkolenie spośród opisanych wcześniej, z uwagi na niezaprzeczalny potencjał uczenia się organizacji poprzez doświadczenie. Taki potencjał wiedzy mają cykliczne szkolenia prowadzone przez IOD, który jest zaznajomiony z rodzajami i specyfiką incydentów ochrony danych osobowych, nie tylko w danej organizacji, ale również w szerokim ujęciu sektorowym.

Warto korzystać z doświadczenia innych podmiotów, a więc czerpać informacje z decyzji organów nadzorczych (zarówno polskiego jak i zagranicznych) oraz wiedzy innych ekspertów (zdobywanej m.in. podczas wymiany doświadczeń w trakcie spotkań stowarzyszeń, konferencji). To naturalne zadanie IOD, ugruntowane w artykule 39 rozporządzenia 2016/679.

Szkolenia a notyfikacja incydentów

Należy mieć na uwadze, iż zwiększenie częstotliwości szkoleń prowadzonych przez IOD nie zmniejszy ilości rejestrowanych incydentów. Szkolenia mają wpływać na rozwój świadomości pracowników dotyczącej między innymi tego, jakie zdarzenia są incydentami ochrony danych osobowych. Paradoksalnie, takich zgłoszeń do IOD oczekujemy coraz więcej. Zwłaszcza, jeżeli dotychczas nie miały one miejsca w ogóle. Czy wypełniony rejestr nie przysporzy nam problemów? Na pewno wątpliwość kontroli pracowników Urzędu Ochrony Danych Osobowych wzbudzi taki rejestr incydentów wewnętrznych, w którym nie jest odnotowany żaden incydent w skali kilku lat prowadzonej działalności.

Jak często przeprowadzać szkolenie z ochrony danych osobowych?

Nie ma jasnych wytycznych w tym zakresie. Poradniki UODO ani Ministerstwa Cyfryzacji nie zawierają takich informacji, mimo że w Internecie napotykamy hasło z kampanii informacyjnej Ministerstwa Cyfryzacji, które „(…) zaleca, aby szkolenia dla pracowników z zakresu ochrony danych osobowych odbywały się co najmniej raz w roku". Widzę konieczność, aby takie szkolenia przeprowadzić więcej niż raz, na początku zatrudnienia. Zdecydowanie warto wykorzystać możliwość uczenia się organizacji na własnym doświadczeniu (zwłaszcza, gdy takie zalecenie otrzymujemy od Prezesa UODO), ale też na doświadczeniu innych podmiotów. Warto również sięgać po ofertę szkoleniową dedykowaną poszczególnym obszarom biznesowym i konkretnym zagadnieniom. Skupić się na tym, co najbardziej nas interesuje.

Agnieszka Dominiak - specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.