Warszawa, 29.09.2020 r.

Dlaczego szkolenia z ochrony danych osobowych są ważne?

Szkolenie pracowników, szczególnie dla jego uczestników, często wydaje się przykrym obowiązkiem. Zdarza się też, że pracownik wyciąga magiczną kartę: „ ja już miałem szkolenie z RODO", dzięki czemu rzekomo nie musi brać w nim udziału ponownie. Czy na pewno?

Dlaczego szkolenie jest ważne?

Podstawowa wiedza personelu z zasad ochrony danych osobowych, to jeden z kluczowych elementów prawidłowego wdrożenia RODO. Każda firma powinna zarówno na początku pracy, jak i okresowo w trakcie wykonywania obowiązków, przypominać pracownikom o takich kwestiach, jak np.:

- zakres danych osobowych i kategorie osób, których dane podlegają wymogom RODO

Zaskakujące, że do tej pory wiele osób błędnie zakłada, że dane jawne, upublicznione np. na firmowych stronach internetowych, na portalach społecznościowych (typu LinkedIn czy Facebook), czy powszechnie dostępnych rejestrach (KRS, CEIDG) nie są tymi samymi danymi osobowymi, co poufne dane zawarte w umowach, teczkach osobowych, czy kartotekach klientów.

Ponadto, z mojej obserwacji wynika, że pracownicy skupiają się w dużej mierze na danych „personalnych", typu imię, nazwisko, PESEL, adres zamieszkania, data urodzenia, jednak z pominięciem innych informacji identyfikujących daną osobę, np. numer umowy, numer faktury, identyfikator w systemie, numer klienta, itp.

Jednym z klasyków, jest także pobłażliwe traktowanie danych dotyczących reprezentantów firm (pełnomocników, członków zarządów, prokurentów, prezesów), czy też osób fizycznych prowadzących działalność gospodarczą. A przecież pamiętajmy, że RODO dotyczy osób fizycznych, bez względu na to, czy jest to osoba prywatna, czy występująca jako profesjonalista.

Brak uświadamiania pracowników o takich podstawowych wydawałoby się kwestiach prowadzi do tego, że w praktyce zbieranie tego typu danych może być w ogóle nie zgłaszane do konsultacji z IOD, przez co cały proces od samego początku jest obarczony ryzykiem niezgodności z RODO (chociażby poprzez brak analizy, czy np. wewnętrznie budowana baza kontaktów zebranych z konferencji, LinkedIn czy innego serwisu ma właściwe podstawy prawne, czy spełniono obowiązek informacyjny, czy ustalono okres przechowywania danych, itp.).

Może się też zdarzyć, że w razie incydentu bezpieczeństwa dotyczącego tych informacji pracownik w ogóle go nie zgłosi, nie mając przekonania, że powinien.

- przypadki, kiedy zbieranie danych nie wymaga zgody, a kiedy na pewno będzie wymagana

To kolejny przykład, kiedy praktyka pracowników to jedno, a RODO (a za nim IOD) – to drugie. Wystarczy pobieżna analiza przykładowych formularzy rejestracyjnych, zakupowych, czy regulaminów usług, albo informacji dotyczących monitoringu wizyjnego, aby się zorientować, że zgoda jest nadmiernie zbierana.

Warto, aby wszyscy pracownicy znali podstawy, z jakich mogą korzystać w przypadku danych, które przetwarzają w swoich działach i że przede wszystkim zgoda nie jest jedyną z nich.

Doszkolenie pracowników z tych podstaw, omówienie przykładów wykorzystania danych i potwierdzenie, na jakich podstawach mogą się opierać w trakcie bieżącej pracy pomoże uniknąć sytuacji, kiedy każdy jeden formularz czy umowa zawiera błędne stwierdzenie, że np. „użytkownik wyraża zgodę na przetwarzanie danych w celu realizacji zamówienia".

- obowiązujące w firmie polityki ochrony danych i powiązane procedury

Mimo opracowania kompletu dokumentów dotyczących zasad ochrony danych osobowych, często okazuje się, że pracownicy o nich po prostu nie wiedzą. Być może nawet mają dostęp do ich treści (np. zostały rozesłane na e-maile, są dostępne w Kadrach albo w Intranecie), ale ich objętość zniechęca do uważnego przeczytania. Taka sytuacja jest dla firmy niebezpieczna, bo oznacza, że wdrożenie RODO kończy się tylko na papierze. **Pracownicy muszą być okresowo szkoleni z tego, jakie są zasady ochrony danych wynikające z RODO i jakie dedykowane procedury w firmie dotyczą tych zasad.**

- reagowanie na incydenty

Aby IOD czy Dział IT prawidłowo ocenili incydent bezpieczeństwa przede wszystkim muszą posiadać o nim (lub o jego podejrzeniu) informację. Informacja taka z kolei może być przekazana tylko przez kogoś kto wie, jakie zdarzenie może być uznane za naruszenie bezpieczeństwa i jaki zakres informacji na pewno będzie potrzebny w minimalnym zakresie. **Zatem każdy pracownik powinien posiadać kompletne informacje o tym, czym jest naruszenie ochrony danych i jak w takim przypadku postępować.**

- zabezpieczenie danych

Chociaż temat wydaje się stary, jak świat, to nadal do wielu naruszeń dochodzi z powodu błędu w zabezpieczeniu lub braku wiedzy, co do prawidłowego zabezpieczenia danych. **Szkolenie personelu z zabezpieczeń danych na miejscu pracy, zagrożeń podczas korzystania z sieci, czy ataków socjotechnicznych skutecznie podniesie poziom wiedzy w tym zakresie**.

Brak uświadamiania pracowników o takich podstawowych wydawałoby się kwestiach to duża luka w systemie ochrony danych osobowych, a tylko wstępne lub okresowe szkolenia mogą zapobiec jej pogłębianiu się.

Jakie szkolenie wybrać i jak je przeprowadzić?

Szkolenie może, ale nie musi być prowadzone przez IOD (może być np. zlecone zewnętrznej firmie z doświadczeniem w tym temacie). To do firmy należy wybór najbardziej efektywnego środka, ale aby szkolenie zapadło uczestnikom w pamięci warto wziąć pod uwagę to, żeby było dostosowane do potrzeb i przeprowadzone ciekawie. Moje propozycje to między innymi:

1. szkolenie stacjonarne dla grup – z podziałem na konkretne działy lub obszary w firmie (np. Kierownictwo, HR, Marketing), aby omawiać tematy dotyczące „codziennego dnia" tych działów/obszarów. Dzięki temu pracownicy nie będą mieć poczucia, że mówimy o teoretycznej abstrakcji
2. szkolenie typu „case study" – omawianie konkretnego przypadku, na praktycznym przykładzie

3. zamiast szkoleń stacjonarnych – przeprowadzenie webinarium. Zdalna forma uczestniczenia w szkoleniu może się okazać atrakcyjna dla pracowników
4. testy wiedzy – warto zakończyć szkolenie testem w zakresie tematu omawianego na szkoleniu
5. interaktywny e-learning z quizem – często przyjemna forma i grafika sprawiają, że wiedza przyswaja się łatwiej i zostaje w głowie na dłużej

Zarówno ja, jak i nasz Zespół iSecure przeprowadziliśmy już wiele szkoleń z zakresu ochrony danych osobowych i chętnie podzielimy się naszym doświadczeniem w tym zakresie ☺

Katarzyna Ułasiuk, Członek Zarządu iSecure Sp. z o.o.