Warszawa, dn. 8.02.2024 r.

Budowanie RODO świadomości w organizacji – bo pracownik stanowi jeden z kluczowych elementów systemu ochrony danych.

Mimo upływu czasu od wdrożenia RODO, temat świadomości pracowników i współpracowników w każdej organizacji jest tematem nadal interesującym.
Pomimo stworzenia części prawno-proceduralnej w organizacji, czyli wdrożenia procedur, dostosowania witryny internetowej, zbudowania rejestrów, obowiązków informacyjnych czy zgód, u osób zarządzających nadal pojawia się niepewność. O szkoleniach i ich rodzajach pisaliśmy już wcześniej tutaj.

W dzisiejszym artykule chce zwrócić uwagę na wagę i możliwości uświadamiania pracowników. Każdy z nas pewnie słyszał, że to człowiek jest najsłabszym ogniwem systemu ochrony danych. Tak może rzeczywiście być, jeśli pracownicy przetwarzają dane osobowe bez świadomości zagrożeń, znajomości zabezpieczeń, czy nawet dbałości o bezpieczeństwo. Samo bowiem wdrożenie powyższego, może okazać się niewystarczające. Aby nasza organizacja była zgodna z RODO, potrzebne jest także zbudowanie wśród pracowników i współpracowników odpowiedniego poziomu wiedzy dotyczącej ochrony danych osobowych.

Definiuje się łatwo, dużo trudniej wprowadzić w życie.

Świadomość pracowników jest kluczem: brak wiedzy, jak zachować się w danej sytuacji, może nie tylko zwolnić pracownika z odpowiedzialności, ale przede wszystkim – stanowić jedną z zasadniczych podatności. Podczas przeprowadzanych audytów w organizacjach, zdarza się zauważać duży brak świadomości. Jak sobie z tym radzić?

Mapowanie procesów, to element, który staram się wdrażać w każdej organizacji. Ważne jest, aby organizacja wprost wskazywała stanowiska i przypisane do niej uprawnienia dostępowe.

Bowiem znaczenie poszczególnych kategorii pracowników dla zgodności z RODO ma nie tylko różny stopień, ale dotyczy też różnych aspektów ochrony danych. Osoby posiadające najszerszy dostęp do danych z reguły są ogniwem najistotniejszym – nie tylko z perspektywy możliwych skutków incydentu, ale też realizacji praw osób, których dane dotyczą. Stąd, uregulowanie tego może pomóc nam w uświadamianiu pracowników.

Nie zapominajmy jednak, że poważny incydent może spowodować właściwie każdy pracownik – nie tylko z braku świadomości, ale czasem także z braku poczucia odpowiedzialności, a nawet złośliwości czy głupoty.

Skutki nieświadomości pracownika częściowo można ograniczyć dzięki rozwiązaniom technicznym, ale zwykle nie będzie to wystarczające. Na przykład, możemy ustawić automatyczne blokowanie ekranu po kilku minutach nieaktywności, ale nie tuż po odejściu pracownika od komputera. Możemy ułatwić korzystanie z książki adresów e-mail, ale nie zablokujemy możliwości błędnego wpisania adresata. Możemy zakupić niszczarki, ale dokumenty nadal można wyrzucić bez ich użycia. Możemy również odpowiednio zabezpieczyć laptopy.

Co jednak jest ważniejsze od powyższego?

Jasna i czytelna informacja - **czego oczekujemy od pracownika na danym stanowisku**. Nie chodzi tutaj o ogólny stopień znajomości przepisów, ale przede wszystkim o odpowiedź, jaka jest rola danego pracownika w ramach systemu ochrony danych. Dobrze przygotowane procedury powalają łatwo ustalić zakresy odpowiedzialności poszczególnych osób. Ważne, aby pracownik wiedział z czym wiążę się dana procedura, w jakim zakresie dotyczy jego obszaru działalności i jakie kroki musi podjąć, jeżeli dojdzie do sytuacji incydentalnej.

Należy **odpowiednio przeszkolić pracownika**. **Zapewnienie prostoty procedur ochrony danych. Zaplanowana** komunikacja na temat wdrożenia ochrony danych to ważny element. Samo przekazanie procedur ochrony danych i ich zapisów może być trudne w odbiorze.
Im bardziej skomplikowana procedura, tym trudniej wyegzekwować jej realizację. Obecnie organizacje przetwarzają ogromną ilość procedur, wytyczny i systemów – dlatego należy ograniczyć objętość wymagań i zapisów, do przyswojenia oraz egzekwowania.

Dobrze działa przygotowanie ,,streszczenia'' dokumentów w wdrożonych w organizacji, napisane prostym i czytelnym językiem. Następnie dedykowane szkolenie dostosowane do danej kategorii pracowników lub udostępnienie szkolenia elektronicznego, gdzie wiedza zostanie sprawdzona testem końcowym.

Informacje na temat ochrony danych powinny docierać także w bardziej przystępny sposób – mogą to być plakaty informacyjne na korytarzach, wysyłany w formie elektronicznej lub wewnętrzny newsletter z zadaniami do wykonania i „przypominajkami" na temat poszczególnych zagadnień.

I bardzo ważne - **bezpieczeństwa nie osiąga się jednorazowo**. Ze względu na zmiany w organizacji, technologii, prawie, a także składzie osobowym zespołu pracowników, efekty jednego szkolenia spadają z upływem czasu. Do budowania świadomości **najlepiej podejść jako do procesu ciągłego**: organizować szkolenia wstępne dla nowych pracowników, prowadzić regularne akcje uświadamiające, a także dokonywać przeglądu funkcjonujących procesów.

Pracownicy **potrzebują narzędzi do osiągnięcia stawianych im wymogów**. Przykładowo, realizacja terminów usunięcia danych czy żądań w zakresie usunięcia danych często wymaga zapewnienia odpowiednich funkcjonalności systemów informatycznych. Wskazuje to na konieczność weryfikacji – najlepiej w toku audytu – jak przyjęte rozwiązania funkcjonują w praktyce i co jest źródłem niedociągnięć.

I w końcu nadanie ochronie danych i RODO odpowiedniej kategorii. Personel organizacji musi wiedzieć, że ochrona danych osobowych jest poważnym zagadnieniem i niesie za sobą konsekwencje. Puste slogany i brak przykładu kadry zarządzającej przekładają się na niski poziom egzekwowania procedur przez pracowników organizacji.

Szkolenia związane z tematyką ochrony danych osobowych są z jednej strony obowiązkiem spoczywającym na administratorach danych, a z drugiej strony są niezwykłą okazją do budowania kultury organizacji. Zdecydowanie warto wykorzystać możliwość uczenia się organizacji na własnym doświadczeniu, skupić się na tym, co najbardziej nas interesuje.

Właściciele firm często nie przykładają wystarczającej wagi do wyedukowania personelu. Warto podkreślić, że powodem naruszeń ochrony danych osobowych jest brak świadomości zagrożeń, jakie wiążą się z przetwarzaniem.

Świadomy pracownik = bezpieczny pracownik!

Olga Skotnicka – specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o., dyrektor operacyjny w iSecure Legal