Warszawa, 09.06.2020 r.

Nieświadomość pracownika szkodzi

Wdrażanie RODO, czy ściślej rzecz biorąc – przestrzeganie wykonywania przepisów w konkretnej firmie, zależy od wielu elementów. Jednym z kluczowych jest zachowanie i świadomość personelu. Dlaczego? Dlatego, że w praktyce błąd po stronie człowieka, choćby niezawiniony, to nadal jeden z najczęstszych powodów braku zgodności z RODO.

Szkolenia bez efektu

Certyfikat po ukończeniu szkolenia. Podpis na liście obecności po szkoleniu. Zaliczony test wiedzy. Uczestnictwo w webinarium. A następnie wiadomość: „W sprawie tej umowy powierzenia muszę Panią skontaktować z naszym ADO, który jest obecnie na spotkaniu" albo „Nie przetwarzamy danych kandydatów do pracy w formie papierowej (tylko Kierownicy proszą nas o wydrukowanie CV, ale cała baza jest w systemie rekrutacyjnym)". Sięgamy wysoko, a czasami brakuje wiedzy elementarnej. Skąd to się bierze? Jednym z powodów są szkolenia zbyt ogólne lub niedostosowane do grupy odbiorców. Podstawy przetwarzania danych powinien znać każdy, ale warto pracownikom Kadr wyjaśnić na szkoleniu, jak ta ochrona danych powinna wyglądać w praktyce konkretnie w pokoju lub archiwum kadrowym, a pracownikom marketingu, jak na przykładzie procesu zbierania zgód na landing page spełnić obowiązki prawne. W przypadku więc ogólnych, wstępnych szkoleń z zasad przetwarzania danych, warto poświęcić chwilę na podanie kilku przykładów „z życia firmy" tak, aby RODO nie było po szkoleniu nadal jedynie abstrakcją, ale konkretnym obszarem do pracy.

Innym „grzechem" może być też próba wyspecjalizowania każdego pracownika w prawie z zakresu ochrony danych. Specjalizacja w tym obszarze zajmuje długie lata (zarówno praktyki, jak i edukacji) i nawet całodniowe szkolenie nie przyniesie takiego efektu. Skuteczne przekazanie wiedzy wszystkim pracownikom wymaga często określenia priorytetów, wskazania kluczowych ryzyk. Innymi słowy – swoistego dawkowania wiedzy.

„To nie moja działka, u nas jest od tego IOD"

Do tej pory, mimo że tak dużo widzi i słyszy się o RODO, część pracowników woli pozostać obok tematu, wychodząc z założenia, że „to ich nie dotyczy". Nie po to wyznaczono IOD, Dział IT, Dział Prawny, żeby teraz jeszcze odpowiadać za ochronę danych – od tego są specjaliści. Brzmi znajomo? W praktyce skuteczne wdrożenie, to praca każdej osoby mającej styczność z danymi osobowymi, a do tego potrzebne jest poczucie odpowiedzialności. Przestrzegamy przed komunikowaniem w firmach, że za wdrożenie RODO odpowiedzialny jest Inspektor Ochrony Danych. Owszem, IOD jest kompetentny w tym obszarze i jego zadaniem jest pomóc wdrożyć RODO m.in. proponując, jak to zrobić, czy informując, jakie są obowiązki. Jednak każda z osób pracująca z danymi osobowymi powinna mieć poczucie, że ochrona danych (a co za tym idzie – realne wdrożenie wymagań RODO) jest również jej zadaniem.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

Procedury, o których w firmie krążą legendy

Nie raz w praktyce zdarzyło mi się spotkać z sytuacją, gdzie mimo złożenia podpisu na oświadczeniu o zapoznaniu się i zobowiązaniu do stosowania funkcjonujących w firmie polityk wewnętrznych, składający ten podpis pracownik nie wie, o jakie polityki chodzi. Brak skutecznego komunikowania w firmie o tym, jakie polityki ochrony danych dotyczą, gdzie się te polityki znajdują do zapoznania się może skutkować tym, że nikt ich nie bierze na poważnie. Pamiętajmy, że polityki ochrony danych to nie stosy mozolnie wypracowanych plików, które mają imponująco wyglądać podczas kontroli. W wewnętrznej procedurze ma być wskazany opis zachowań, jakich oczekujemy od pracowników oraz spis realnych zasad, jakie w firmie wprowadzamy. A to wszystko ma być **jasne i dostępne dla pracownika**.

Światełko w tunelu

Brak świadomości pracowników jest błędem, który stosunkowo łatwo można naprawić i to bez ponoszenia dodatkowych kosztów. Można spróbować kilku metod, np.:

1. Mailowe akcje edukacyjne – czyli wysyłanie regularnie krótkich, treściwych komunikatów na konkretny temat. Prostym językiem, a nawet w przejrzystej, graficznej formie.
2. Działania prewencyjne w zakresie incydentów – jeżeli w firmie doszło do naruszenia lub o takim naruszeniu wiadomo z doniesień medialnych, warto wyjaśnić pracownikom, na czym ono polegało i jak postąpić, aby nie miało ono miejsca w przyszłości. Warto też na konkretnym przypadku omówić, jak postąpić w przypadku podejrzenia czy wiedzy o naruszeniu (przypomnienie o procedurze reagowania na incydenty w praktyce).
3. Audyty okresowe powdrożeniowe – warto wybrać sobie jeden konkretny obszar, np. strona internetowa lub monitoring i poddać go wewnętrznemu audytowi. Większa szansa, że właściciele danego procesu skupią swoją uwagę na konkretnych aspektach i przełożą tak nabytą wiedzę na analogiczne przypadki w przyszłości.
4. Informowanie o zauważonym błędzie wszystkich pracowników i wskazywanie poprawnego działania – nie chodzi oczywiście o napiętnowanie danego pracownika, ale o komunikat typu: „Zauważamy, że nadal w praktyce zdarzają się przypadki negocjowania umów z dostawcą bez weryfikacji, czy przyszły kontrahent jest zgodny z RODO. Przypominamy o takim obowiązku, ponieważ wynika on z wewnętrznej procedury zatwierdzonej przez Zarząd. Pamiętajcie, że zgodnie z nią powinniśmy […]”
5. Interaktywny e-learning z quizem/testem wiedzy – często przyjemna forma i grafika sprawiają, że wiedza przyswaja się łatwiej i zostaje w głowie na dłużej.

Nie od razu Rzym zbudowano, dlatego nie oczekujemy efektów po jednym tygodniu. Ale zapewniam, że regularne, systematyczne działanie przynosi spodziewane efekty, dzięki czemu każda firma może uniknąć konsekwencji w postaci kary PUODO za działanie lub zaniechanie, które wynika wyłącznie z nieświadomości pracownika.

Katarzyna Ułasiuk, iSecure Sp. z o.o.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł