Ochrona danych osobowych od A do Z w 16 krokach

Fragment

Część I
Przewodnik od A do Z

Rozdział 1. Przygotowanie do kursu

1. Pięć motywatorów, aby zadbać o twój system ochrony danych

1.1. Katalog

1. Odpowiedzialność
2. Reputacja
3. Oszczędzanie czasu
4. Efektywność kosztowa
5. Szacunek dla osób fizycznych

Gratuluję rozpoczęcia kursu! Jak obiecywałem, od teraz uczysz się przez działanie – a jeśli naprawdę zrealizujesz instrukcje, pod koniec tego kursu osiągniesz już imponujące postępy ze swoim systemem ochrony danych.

Od teraz mówię już tylko o tym, jakie byłyby moje kroki, gdybyś zatrudnił mnie do opieki nad twoim systemem ochrony danych. Podążaj za mną!

Zacznijmy od podstawowego pytania: po co dbać o ochronę danych i prywatność? Dlaczego ty, twój szef oraz każdy współpracownik miałby o nie dbać? Cóż, istnieje 5 głównych motywatorów: odpowiedzialność, reputacja, oszczędność czasu, opłacalność i szacunek dla osób, których dane dotyczą.

Zatem pierwsze pytanie, na które musisz odpowiedzieć, brzmi: jak ważna jest ochrona danych dla ciebie, twojej organizacji, kierownictwa i personelu? A jak ważna powinna być? W tym zawiera

się wszystko. Nie daj się zwieść – bez poparcia, projekt ochrony danych w twojej firmie będzie ignorowany.

1.2. Motywator 1: odpowiedzialność

- **Unikanie kar administracyjnych** (sprawdź listę i podsumowania kar nałożonych na podstawie prawa UE na stronie enforcementtracker.com, dostęp: 13.3.2021 r.)
- **Unikanie pozwów, odszkodowań i ugód** (ludzie mogą wystąpić przeciw tobie z własnymi roszczeniami)
- **Unikanie postępowań dyscyplinarnych lub nawet zarzutów karnych** (także pracownicy i współpracownicy są odpowiedzialni)

Kary finansowe

Zacznijmy od odpowiedzialności. W Unii Europejskiej odbyło się duże odliczanie do 25.5.2018 r., kiedy weszło w życie RODO. Od tej pory, większość podmiotów przetwarzających dane osobowe podlega karze finansowej do 20 mln euro, lub w przypadku przedsiębiorstwa – do 4% jego całkowitego rocznego światowego obrotu (art. 83 RODO). Skutkiem wejścia w życie RODO były gigantyczne kary, takie jak kara 204 mln euro dla British Airways, 110 mln euro dla Marriott International, ale też dotkliwe kary dla zwykłych przedsiębiorstw, jak 644 tys. euro dla polskiego sklepu online.

Kary dotknęły także niewielkich przedsiębiorstw, takich jak austriacka restauracja z kebabem, która stosowała monitoring bez podstawy prawnej. Rekomenduję regularnie sprawdzać stronę enforcementtracker.com z listą kar i związanych z nimi kluczowych faktów – pozwala sortować kary po ich wielkości i zobaczyć, że wyciek, utrata danych lub brak wystarczających zabezpieczeń najczęściej pociągają za sobą największą odpowiedzialność.

Kary finansowe na terenie poza UE

Na terenie poza UE kary mogą być nawet wyższe. Na przykład agencja kredytowa Equifax musiała zapłacić 700 mln dolarów za naruszenie ochrony danych w ramach ugody z U.S. Federal Trade Commission. Nie było to unijne 4% rocznego obrotu, ale aż 20% przychodu Equifax za rok 2018.

Amerykańska FTC nałożyła również gigantyczną karę 4,49 mld euro na Facebook, w związku ze skandalem Cambridge Analytica. Czy to oznacza, że USA ustanowiły swój standard ochrony danych wyżej od unijnego RODO? Oznacza to, że niezależnie skąd jesteś – jeśli ludzie poniosą szkodę, gdy ich prawa związane z danymi osobowymi, które przetwarzałeś, zostaną naruszone, to będą dążyć do tego, abyś poniósł odpowiedzialność.

Odpowiedzialność pracowników

Zatem pierwszy motywator to chęć uniknięcia kar i odpowiedzialności finansowej. Nie dotyczy to jedynie podmiotów jako całości. Pracownicy również mogą zostać pociągnięci do odpowiedzialności, a już teraz mają miejsce przestępstwa, takie jak bezprawne przetwarzanie danych osobowych lub kradzież tożsamości.

1.3. Motywator 2: reputacja

- **Ochrona zaufania** konsumentów, pracowników i kontrahentów
- **Unikanie naruszeń**, które należy zgłosić organom i osobom fizycznym
- **Unikanie skarg i negatywnych opinii**

Drugim motywatorem jest reputacja twojej firmy. W razie naruszenia, możesz nie tylko otrzymać karę od organów, ale jednocześnie stracić część zaufania konsumentów, pracowników lub kontrahentów. Powiedzmy, że twoja firma używa usług chmurowych stron trzecich do przechowywania danych swoich klientów. Pewnego dnia, u dostawcy chmury dochodzi do utraty danych. Musisz poinformować klientów i pracować nad obsługą wielu skarg. Czy poleciłbyś tego dostawcę chmury? Na pewno nie.

Bezpieczeństwo informacji

Jeżeli informacje znaczą wiele dla twojej firmy, to ich bezpieczeństwo znaczy wiele dla twojej reputacji. Jeśli prowadzisz firmę zajmującą się ochroną danych, myślę, że ostatnią rzeczą, którą chcesz zobaczyć, jest poważne naruszenie danych w twojej firmie.

1.4. Motywator 3: oszczędzanie czasu

- **Planowanie i kontrola zamiast chaosu** (nie zwlekaj do czasu wystąpienia naruszenia, skargi lub kontroli)
- **Unikanie marnowania lub podwójnego wysiłku** (oprzyj się na ustaleniach, produktach i zarządzaniu projektem)
- **Maksymalizacja skutków** (spróbuj rozwiązać kilka problemów jednym działaniem)

Myślę, że oszczędzanie czasu to najczęściej ignorowany motywator, który docenisz w trakcie tego kursu. O wiele łatwiej i szybciej jest stworzyć dobre rozwiązania od początku, niż oceniać i poprawiać rozwiązania już istniejące. I tak będziesz potrzebował dobrego systemu ochrony danych, dlatego lepiej jest go mieć, zanim wystąpi jakikolwiek incydent lub postępowanie.

Jeśli twoja firma zatrudniła kogoś, kto zdecydowanie nie wykonał dobrej pracy , najprawdopodobniej bardziej efektywne będzie podążanie za tym kursem tak, jakby twoja firma dopiero zaczynała wprowadzać system ochrony danych. Jeśli natomiast twoja firma wykonała już pewien postęp, nauczę cię, jak najlepiej to wykorzystać.

1.5. Motywator 4: efektywność kosztowa

- Celuj w dobry **zwrot z inwestycji – ROI** (jasno określ i weryfikuj wyniki projektu)
- Niektóre firmy **straciły setki tysięcy** na nieodpowiednich ekspertów
- **Większość ukaranych spółek zapłaciła wcześniej za projekt zgodności**, ale nie był on efektywny

Motywator 4 jest ściśle powiązany z motywatorem 3, ale bezpośrednio dotyczy pytania, jak dużo pieniędzy musisz wydać, aby otrzymać dobry system ochrony danych. Znam firmy, które wydały

setki tysięcy na nieodpowiednich ekspertów, którzy dużo mówili, ale prawie nic nie zrobili. Tak dzieje się, gdy myślisz w ten sposób: z naszymi rozmiarami, prędzej czy później dostaniemy milionową karę. Lepiej więc zapłacić 100 tys. dolarów i pozwolić wziąć odpowiedzialność ekspertom.

Cóż, jeśli spojrzysz na decyzje o nałożeniu kar, okazuje się, że większość ukaranych firm miała projekt ochrony danych, klauzule, a nawet audyty. Zatem zapłaciły zarówno za ekspertów, jak i kary. Ktoś zapłacił, ktoś zarobił, a sytuacja nie uległa zmianie.

Czy to oznacza, że lepiej po prostu czekać na karę? Jasne, że nie. Znaczy to jednak, że spółka powinna zweryfikować, czy projekt osiągnął swoje cele, a jeśli nie – wyciągnąć konsekwencje.

1.6. Motywator 5: szacunek dla osób fizycznych

- **Klient ma zawsze rację –** dotyczy to także prywatności
- W razie możliwych problemów z prywatnością, **twój klient lub partner może rozważyć przeniesienie się do konkurencji**
- Jeśli kiedykolwiek zmieniałeś swoje ustawienia prywatności, rozumiesz ten punkt

Ostatnim z motywatorów do wskazania jest szacunek dla osób, których dane dotyczą – w szczególności dla klientów. Klient ma zawsze rację i dotyczy to także jego lub jej prywatności. Jeśli konsument uważa, że mogą wystąpić problemy z prywatnością, on lub ona może nawet rozważyć przeniesienie się do twojej konkurencji.

Czy sam nie jesteś konsumentem? Jeśli kiedykolwiek zmieniałeś swoje ustawienia prywatności, znasz powód. Jest to to samo uczucie, gdy ktoś zadaje zbyt wiele pytań na temat twojego życia osobistego. Nawet jeśli nie przejmowałbyś się tym, niektórzy konsumenci mogą mieć takie same odczucia odnośnie do twojej polityki zbierania danych.

Jak wspomniałem, wszystkim czego potrzebujesz są wsparcie kierownictwa, czas i zasoby. A wszystko zaczyna się od wsparcia

kierownictwa – jeśli jest motywacja po jego stronie, to jesteś na dobrej drodze do otrzymania odpowiedniej ilości czasu, zasobów i okazji do wykonania pracy oraz zaangażowania innych członków personelu.

1.7. Wsparcie od kierownictwa i interesariuszy

- Upewnij się, że **twój zarząd chce** mieć system ochrony danych (ochrona danych wymaga rzeczywistych działań i budżetu)
- Omawiam cały projekt, ale twój zarząd **może wybrać tylko niektóre usługi** (np. audyt, dokumentację lub inspektora ochrony danych)
- Od pierwszego dnia, pozyskuj poparcie od każdego, w tym od pracowników. Ich pomysły i wkład są świetne
- Im bardziej pomożesz im z ich obowiązkami, tym bardziej pomogą Tobie
- **Użyj motywatorów**, o których się dowiedziałeś, i stale szukaj nowych

Podejście holistyczne

Czasem wsparcie kierownictwa nie jest pełne. Proszą cię o zajęcie się priorytetami i odłożenie reszty na później. Uświadom ich, że holistyczne podejście jest najbardziej efektywne, natomiast jeśli odmówią – zaakceptuj to.

Traktuj jednak nawet najmniejszą usługę jako część tego, o czym uczysz się na tym kursie. Jest to najlepszy sposób, aby sprawić, że każdy wysiłek jest krokiem w stronę pełnoprawnego systemu ochrony danych, który omawiamy.

Wsparcie personelu

Podczas gdy wsparcie twojego kierownictwa jest nieodzowne do startu, od razu myśl także o wsparciu od personelu.

Postaraj się być osobą pomocną, dającą większe bezpieczeństwo i pewność. Zanim się pojawiłeś, pracownicy prawdopodobnie męczyli się z ochroną danych i wdrażaniem klauzul bez odpowiedniej wiedzy. Traktowali to jak dodatkowe obciążenie, z którym nie wiadomo, jak sobie poradzić.

Zawsze pytaj, jak możesz im pomóc, czego potrzebują, co jest niejasne i czego brakuje, jeśli chodzi o ochronę danych. Jeśli zobaczą, że stosujesz 5 naszych motywatorów, jest to najlepszy sposób, aby zmotywować także ich.

2. 10 różnic między firmą niedbającą o prywatność a twoimi celami

2.1. Uwagi wstępne

1. Cele przetwarzania danych
2. Zakres przetwarzanych danych
3. Weryfikacja i aktualizacja
4. Przechowywanie
5. Prawdopodobieństwo naruszenia
6. Waga naruszenia
7. Prawa osób fizycznych
8. Formalna zgodność
9. Przejrzystość
10. Dowody

Istnieje 10 głównych kryteriów pozwalających jasno określić, jak twój system ochrony danych funkcjonuje, i czy w ogóle istnieje. Aby z nich skorzystać, po prostu zapytaj kierownictwo, czy te kwestie zostały zaadresowane. Jeśli nie, przed tobą najprawdopodobniej trochę pracy.

Zapamiętaj jednak ten moment. Na koniec projektu, zadasz dokładnie takie same pytania. To na pewno pokaże, jak duży postęp zrobiłeś.

Spójrzmy bliżej na każdą z tych 10 różnic.