

Ochrona danych osobowych od A do Z w 16 krokach

Przejdź do produktu na ksiegarnia.beck.pl

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
 - 1.2. Motywator 1: odpowiedzialność
 - 1.3. Motywator 2: reputacja
 - 1.4. Motywator 3: oszczędzanie czasu
 - 1.5. Motywator 4: efektywność kosztowa
 - 1.6. Motywator 5: szacunek dla osób fizycznych
 - 1.7. Wsparcie od kierownictwa i interesariuszy
2. 10 różnic między firmą niedbającą o prywatność a twoimi celami
 - 2.1. Uwagi wstępne
 - 2.2. Różnica 1: cele przetwarzania danych
 - 2.3. Różnica 2: zakres przetwarzanych danych osobowych
 - 2.4. Różnica 3: weryfikacja i aktualizacja
 - 2.5. Różnica 4: przechowywanie
 - 2.6. Różnica 5: prawdopodobieństwo naruszenia bezpieczeństwa
 - 2.7. Różnica 6: waga naruszenia
 - 2.8. Różnica 7: prawa osób fizycznych
 - 2.9. Różnica 8: formalna zgodność
 - 2.10. Różnica 9: przejrzystość
 - 2.11. Różnica 10: dowody
3. Dlaczego kontekst przetwarzania danych ma znaczenie?
 - 3.1. Organizacja, którą będziesz obsługiwać
 - 3.2. Znaczenie kontekstu organizacji
 - 3.3. Gdzie zapisywać odpowiedzi?
 - 3.4. Krótki opis działalności organizacji
 - 3.5. Właściwe prawo i standardy
 - 3.6. Jak uwzględnić lokalne i szczegółowe przepisy?
 - 3.7. Szacowana liczba osób, których dane dotyczą
 - 3.8. Lokalizacje, gdzie dane są przetwarzane
 - 3.9. Jak będzie wyglądać twój projekt?

Część I. Przewodnik od A do Z

4. Cztery fazy – 16 kroków
 - 4.1. Wprowadzenie
 - 4.2. Faza 1: zidentyfikuj
 - 4.3. Faza 2: oceń
 - 4.4. Faza 3: wdrażaj
 - 4.5. Faza 4: stosuj
5. Zaczynij działać!
 - 5.1. Wprowadzenie
 - 5.2. Zespół ds. prywatności
 - 5.3. Model zarządzania
 - 5.4. Jak przygotować projekt?
 - 5.5. Spotkanie inauguracyjne
 - 5.6. Po spotkaniu inauguracyjnym
 - 5.7. Wiadomość do wysłania do rozmówców (procesy)
 - 5.8. Wiadomość do wysłania do rozmówców (zasoby)
 - 5.9. Wiadomość do wysłania do rozmówców (ogólne obowiązki)
 - 5.10. Twoja lista rzeczy do zrobienia (przygotuj się do startu)

Rozdział 2. Faza 1: Zidentyfikuj

1. Krok 1: Zidentyfikuj cele przetwarzania danych
 - 1.1. Tryb działania
 - 1.2. Procesy i przetwarzanie
 - 1.3. Typowe procesy (administrator)
 - 1.4. Typowe procesy (procesor)
 - 1.5. Cele a procesy
 - 1.6. Czyje są cele?
 - 1.7. Których kwestionariuszy używać?
 - 1.8. Operacje przetwarzania (kwestionariusz administratora)
 - 1.9. Współadministratorzy (kwestionariusz administratora)
 - 1.10. Cele przetwarzania (kwestionariusz administratora)
 - 1.11. Typowe cele (dodaj więcej szczegółów, jeśli to możliwe)
 - 1.12. Administratorzy (kwestionariusz procesora)
 - 1.13. Operacje i cele przetwarzania (kwestionariusz procesora)
 - 1.14. Twoja lista rzeczy do zrobienia (krok 1)
2. Krok 2: Zidentyfikuj szczegóły przetwarzania danych
 - 2.1. Kategorie podmiotów danych (kwestionariusz administratora)
 - 2.2. Typowe kategorie podmiotów danych
 - 2.3. Kategorie danych osobowych (kwestionariusz administratora)
 - 2.4. Typowe kategorie „zwykłych” danych osobowych
 - 2.5. Szczególne kategorie danych osobowych
 - 2.6. Kategorie odbiorców (kwestionariusz administratora)
 - 2.7. Typowe kategorie odbiorców
 - 2.8. Przekazywanie danych poza Europejski Obszar Gospodarczy (kwestionariusz administratora)

- 2.9. Typowe przypadki przekazywania poza EOG
- 2.10. Planowane terminy usunięcia danych (kwestionariusz administratora)
- 2.11. Typowe terminy usunięcia danych
- 2.12. Ogólny opis środków bezpieczeństwa (zarówno kwestionariusze administratora, jak i procesora)
- 2.13. Przekazywanie danych poza EOG (kwestionariusz procesora)
- 2.14. Udzielanie gwarancji administratorom (kwestionariusz procesora)
- 2.15. Twoja lista rzeczy do zrobienia (krok 2)
- 3. Krok 3: Zidentyfikuj zasoby
 - 3.1. Tryb działania
 - 3.2. Jak pogrupować zidentyfikowane zasoby?
 - 3.3. Lokalizacje i obszary
 - 3.4. Typowe zasoby (lokalizacje i obszary)
 - 3.5. Typowe zabezpieczenia (lokalizacje i obszary)
 - 3.6. Sprzęt
 - 3.7. Typowe zasoby (sprzęt)
 - 3.8. Typowe zabezpieczenia (sprzęt)
 - 3.9. Sieci i serwery
 - 3.10. Typowe zasoby (sieci i serwery)
 - 3.11. Typowe zabezpieczenia (sieci i serwery)
 - 3.12. Strony internetowe
 - 3.13. Typowe zasoby (strony internetowe)
 - 3.14. Typowe zabezpieczenia (strony internetowe)
 - 3.15. Oprogramowanie
 - 3.16. Typowe zasoby (oprogramowanie)
 - 3.17. Typowe zabezpieczenia (oprogramowanie)
 - 3.18. Pliki elektroniczne (nieustrukturyzowane)
 - 3.19. Typowe zasoby (pliki elektroniczne)
 - 3.20. Typowe zabezpieczenia (pliki elektroniczne)
 - 3.21. Wydrukowane dokumenty
 - 3.22. Typowe zasoby (wydrukowane dokumenty)
 - 3.23. Typowe zabezpieczenia (wydrukowane dokumenty)
 - 3.24. Personel
 - 3.25. Typowe zasoby (personel)
 - 3.26. Typowe zabezpieczenia (personel)
 - 3.27. Inne
 - 3.28. Twoja lista rzeczy do zrobienia (krok 3)
- 4. Krok 4: Zidentyfikuj właścicieli procesów i zasobów
 - 4.1. Właściciele procesów i zasobów
 - 4.2. Właściciel procesu – typowe obowiązki
 - 4.3. Właściciel zasobu – typowe obowiązki

Część I. Przewodnik od A do Z

4.4. Twoja lista rzeczy do zrobienia (krok 4)

Rozdział 3. Faza 2: ocena

1. Wstęp: faza oceny
 - 1.1. Tryb działania
 - 1.2. Rejestr czynności przetwarzania (kwestionariusze administratora)
 - 1.3. Rejestr wszystkich kategorii czynności przetwarzania (kwestionariusze procesora)
2. Krok 5: Ocena procesy administratora
 - 2.1. Cel 1: przetwarzaj dane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach
 - 2.1.1. Zasada ograniczenia celu (kwestionariusz administratora)
 - 2.1.2. Zasada zgodności z prawem (kwestionariusz administratora)
 - 2.1.3. Podstawy prawne udostępniania danych (kwestionariusz administratora)
 - 2.2. Cel 2: przetwarzaj tylko te kategorie danych, które są niezbędne w twoim celu. Zasada minimalizacji danych (kwestionariusz administratora)
 - 2.3. Cel 3: upewnij się, że dane osobowe są prawidłowe i aktualne. Zasada prawidłowości (kwestionariusz administratora)
 - 2.4. Cel 4: usuwaj dane osobowe, które nie są już niezbędne w żadnym celu. Zasada ograniczenia przechowywania (kwestionariusz administratora)
 - 2.5. Cel 5: chroń dane osobowe przed naruszeniem bezpieczeństwa
 - 2.6. Cel 6: chroń osoby fizyczne przed naruszeniem ich praw
 - 2.6.1. Obowiązek przeprowadzenia DPIA (kwestionariusz administratora)
 - 2.6.2. Zagrożenia dla osób fizycznych (kwestionariusz administratora)
 - 2.7. Cel 7: przygotuj się do obsługi żądań osób fizycznych
 - 2.8. Cel 8: spełnij wszystkie formalne wymogi prawne
 - 2.8.1. Współadministratorzy (kwestionariusz administratora)
 - 2.8.2. Typowe podatności (procesory)
 - 2.8.3. Procesory zapewniający gwarancje zgodności (kwestionariusz administratora)
 - 2.8.4. Procesory zobowiązali się przestrzegać wszystkich obowiązków z RODO (kwestionariusz administratora)
 - 2.8.5. Zgodność z prawem przekazań poza EOG (kwestionariusz administratora)
 - 2.9. Cel 9: podawaj osobom fizycznym wszystkie niezbędne informacje o ich prawach
 - 2.9.1. Zasada przejrzystości (kwestionariusz administratora)

- 2.9.2. Podawanie wszystkich wymaganych informacji (kwestionariusz administratora)
- 2.9.3. Terminowe podawanie informacji (kwestionariusz administratora)
- 2.9.4. Cel 10: osiągnij rozliczalność – zdolność do wykazania zgodności
- 2.10. Twoja lista rzeczy do zrobienia (krok 5)
- 3. Krok 6: Oceń procesy procesora
 - 3.1. Cel 1: przetwarzaj dane tylko w ramach umowy z administratorem
 - 3.2. Cel 2: udziel administratorowi gwarancji ochrony danych. Udzielanie gwarancji administratorom (kwestionariusz procesora)
 - 3.3. Cel 3: nie angażuj dalszego procesora bez zgody administratora i takich samych obowiązków
 - 3.4. Cel 4: zapewnij poufność wszystkim osobom upoważnionych do przetwarzania danych osobowych
 - 3.5. Cel 5: chroń dane osobowe przed naruszeniem bezpieczeństwa
 - 3.6. Cel 6: pomagaj administratorowi z żądaniami osób fizycznych
 - 3.7. Cel 7: pomagaj administratorowi wypełniać inne obowiązki
 - 3.8. Cel 8: wykaż administratorowi realizację obowiązków procesora
 - 3.9. Twoja lista rzeczy do zrobienia (krok 6)
- 4. Krok 7: Oceń bezpieczeństwo informacji
 - 4.1. Kryteria dla oceny bezpieczeństwa informacji
 - 4.2. Tryb działania (ocena bezpieczeństwa informacji)
 - 4.3. Przypadki wysokiego prawdopodobieństwa oraz ocena integralności i poufności
 - 4.4. Lokalizacje i obszary
 - 4.4.1. Typowe naruszenia bezpieczeństwa (lokalizacje i obszary)
 - 4.4.2. Typowe podatności (lokalizacje i obszary)
 - 4.5. Sprzęt
 - 4.5.1. Typowe naruszenia bezpieczeństwa (sprzęt)
 - 4.5.2. Typowe podatności (sprzęt)
 - 4.6. Sieci i serwery
 - 4.6.1. Typowe naruszenia bezpieczeństwa (sieci i serwery)
 - 4.6.2. Typowe podatności (sieci i serwery)
 - 4.7. Strony internetowe
 - 4.7.1. Typowe naruszenia bezpieczeństwa (strony internetowe)
 - 4.7.2. Typowe podatności (strony internetowe)
 - 4.8. Oprogramowanie
 - 4.8.1. Typowe naruszenia bezpieczeństwa (oprogramowanie)
 - 4.8.2. Typowe podatności (oprogramowanie)

Część I. Przewodnik od A do Z

- 4.9. Pliki elektroniczne
 - 4.9.1. Typowe naruszenia bezpieczeństwa (pliki elektroniczne)
 - 4.9.2. Typowe podatności (pliki elektroniczne)
- 4.10. Wydrukowane dokumenty
 - 4.10.1. Typowe naruszenia bezpieczeństwa (wydrukowane dokumenty)
 - 4.10.2. Typowe podatności (wydrukowane dokumenty)
- 4.11. Personel
 - 4.11.1. Typowe naruszenia bezpieczeństwa (personel)
 - 4.11.2. Typowe podatności (personel)
- 4.12. Inne zasoby
- 4.13. Twoja lista rzeczy do zrobienia (krok 7)
- 5. Krok 8: Oceń ogólne obowiązki
 - 5.1. Inspektor ochrony danych lub odpowiednik
 - 5.1.1. Inspektor ochrony danych – wyznaczenie (kwestionariusz ogólnych obowiązków)
 - 5.1.2. Inspektor ochrony danych – status (kwestionariusz ogólnych obowiązków)
 - 5.1.3. Inspektor ochrony danych – zadania (kwestionariusz ogólnych obowiązków)
 - 5.2. Zarządzanie naruszeniem i raportowanie
 - 5.3. *Privacy by design & by default*
 - 5.4. Prawa osób fizycznych
 - 5.4.1. Prawo dostępu
 - 5.4.2. Prawo do sprostowania
 - 5.4.3. Prawo do usunięcia danych (do bycia zapomnianym)
 - 5.4.4. Prawo do ograniczenia przetwarzania
 - 5.4.5. Obowiązek powiadomienia o sprostowaniu, usunięciu lub o ograniczeniu przetwarzania
 - 5.4.6. Prawo do przenoszenia danych
 - 5.4.7. Prawo do sprzeciwu
 - 5.4.8. Prawo, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu
 - 5.5. Polityki i procedury
 - 5.6. Obowiązki i świadomość pracowników
 - 5.7. Podsumowanie dla kierownictwa i ocena ryzyka
 - 5.8. Twoja lista rzeczy do zrobienia (krok 8)

Rozdział 4. Faza 3: wdrażaj

- 1. Krok 9: Modeluj procesy administratora
 - 1.1. Wstęp: faza wdrożenia
 - 1.2. Dostosuj zbieranie danych
 - 1.3. Dostosuj zakres przetwarzania danych
 - 1.4. Przygotuj klauzule informacyjne

- 1.5. Zaktualizuj umowy
- 1.6. Twoja lista rzeczy do zrobienia (krok 9)
2. Krok 10: Modeluj procesy procesora
 - 2.1. Dostosuj zakres przetwarzania
 - 2.2. Dostosuj komunikację z administratorem i podmiotami danych
 - 2.3. Dostosuj umowy
 - 2.4. Twoja lista rzeczy do zrobienia (krok 10)
3. Krok 11: Zarządzaj ryzykami bezpieczeństwa
 - 3.1. Wstęp: zarządzanie ryzykami bezpieczeństwa
 - 3.2. Ogólne cele, standardy i kontekst bezpieczeństwa
 - 3.3. Przywództwo, role i obowiązki
 - 3.4. Rejestr zasobów, analiza i zarządzanie ryzykiem
 - 3.5. Zarządzanie zasobami, obsługa nośników i klasyfikacja informacji
 - 3.6. Praca mobilna, praca z domu, prywatne urządzenia i wykorzystanie w celach prywatnych
 - 3.7. Zarządzanie upoważnieniami i kontrolą dostępu
 - 3.8. Bezpieczeństwo fizyczne i środowiskowe
 - 3.9. Rejestrowanie zdarzeń oraz monitorowanie podatności i wykorzystania
 - 3.10. Szyfrowanie
 - 3.11. Relacje z dostawcami
 - 3.12. Bezpieczeństwo sieci i przesyłanie informacji
 - 3.13. Oprogramowanie – zabezpieczenia i zarządzanie podatnościami
 - 3.14. Rekrutacja, zatrudnienie, zakończenie zatrudnienia i obowiązki użytkownika końcowego
 - 3.15. Zarządzanie projektami, wyjątki i nietypowe zasoby
 - 3.16. Zarządzanie naruszeniami
 - 3.17. Ciągłość działania i odzyskiwanie po awarii
 - 3.18. Przeglądy i ocena skuteczności
 - 3.19. Twoja lista rzeczy do zrobienia (krok 11)
4. Krok 12: Przestrzegaj ogólnych obowiązków
 - 4.1. Inspektor ochrony danych lub odpowiednik
 - 4.2. Zarządzanie naruszeniem i raportowanie
 - 4.3. *Privacy by design*
 - 4.4. Prawa osób fizycznych
 - 4.5. Obowiązek konsultacji z organem nadzorczym
 - 4.6. Twoja lista rzeczy do zrobienia (krok 12)

Rozdział 5. Faza 4: stosuj

1. Krok 13: Przygotuj ogólne polityki
 - 1.1. Wstęp: faza stosowania
 - 1.2. Dlaczego ogólne polityki mają być użyteczne?
 - 1.3. Jakie aspekty powinny obejmować polityki?

Część I. Przewodnik od A do Z

- 1.4. Jak przygotować ogólne polityki?
- 1.5. Relacja ze standardowymi procedurami postępowania (SOP)
- 1.6. Twoja lista rzeczy do zrobienia (krok 13)
2. Krok 14: Przygotuj procedury (SOP)
 - 2.1. Ogólna SOP
 - 2.2. Standardowe procedury operacyjne dla procesów administratora
 - 2.3. Standardowe procedury operacyjne dla procesów procesora
 - 2.4. Standardowe procedury operacyjne dla zasobów
 - 2.5. Twoja lista rzeczy do zrobienia (krok 14)
3. Krok 15: Przyjmij, opublikuj i przeszkol
 - 3.1. Przyjmij dokumentację ochrony danych
 - 3.2. Opublikuj dokumentację ochrony danych
 - 3.3. Przeszkol pracowników i współpracowników
 - 3.4. Twoja lista rzeczy do zrobienia (krok 15)
4. Krok 16: Egzekwuj, utrzymuj i rewiduj
 - 4.1. Egzekwuj wewnętrzne obowiązki
 - 4.2. Utrzymaj zgodność i aktualność twojego systemu
 - 4.3. Regularnie rewiduj i ulepszaj twój system ochrony danych
 - 4.4. Twoja lista rzeczy do zrobienia (krok 16)

Rozdział 6. Podsumowanie

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

Gratuluje 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. Po-dążaj 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 dotkliwie 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.

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.

Odpowiedzialność pracowników

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 polecilibyś tego dostawcę chmury? Na pewno nie.

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.

Bezpieczeństwo informacji

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. Znaczący 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 wspominałem, 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 zobaczysz, 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.

[Przejdź do księgarni →](#)