

Ochrona prywatności w organizacji. O co zadbać?

W TYM WYDANIU:

Zarządzanie bezpieczeństwem danych osobowych jako centralny element ISMS w przedsiębiorstwie

2

Compliance – czy jest tak bardzo potrzebne w przedsiębiorstwie i dlaczego? Wchodzimy w szczegóły

9

Prasówka

13

Kary z Polski i świata

16



Patrycja Żarska-Cynk

Zarządzanie bezpieczeństwem danych osobowych jako centralny element ISMS w przedsiębiorstwie

Popularyzacja technologii cyfrowych, przetwarzania w chmurze i internet rzeczy oznacza gromadzenie, przechowywanie i przetwarzanie przez organizacje ogromnej ilości danych, w szczególności danych osobowych. Dane osobowe w tych realiach nie ograniczają się już tylko do dokumentacji kadrowej czy finansowej. Współczesne systemy wykorzystują różnorodne informacje, które umożliwiają efektywne zarządzanie personelem i skuteczne angażowanie zarówno klientów biznesowych, jak i indywidualnych konsumentów.

Czy zastanawialiście się, jakie dane osobowe zawierają dokumenty pracownika, jakie dane zawiera ich zdigitalizowana wersja? A co więcej możemy dowiedzieć się o stylu pracy, zainteresowaniach czy nawet danych geolokalizacyjnych, poprzez narzędzia takie jak Microsoft 365 czy Google Workspace? Co może nam powiedzieć oprogramowanie komputera pokładowego samochodu ciężarowego? Wielu z nas nie zdaje sobie sprawy z wielowymiarowości informacji, które mogą być o nas gromadzone i jakie tajemnice naszego codziennego życia mogą zostać odkryte w cyfrowym świecie.

Żyjemy w otoczeniu pełnym informacji, a naruszenie ich bezpieczeństwa niesie za sobą ryzyko dla człowieka, którego te dane dotyczą. RODO, nie pozwala zapomnieć biznesowi, że utrata

poufności czy integralności tych danych, to także wymierne straty biznesowe, a ryzyka utraty bezpieczeństwa w przetwarzaniu tych danych wymagają identyfikacji i kontroli.

Standardy bezpieczeństwa danych – klucz do wzmocnienia organizacji

Standardy bezpieczeństwa danych

W świecie cyfrowej transformacji, gdzie dane są złotem, niezależnie od branży, bezpieczne przechowywanie i przetwarzanie danych to klucz do zaufania klientów i trwałego sukcesu na rynku. Firmy świadome wartości swoich danych oraz danych klientów, sięgają po gotowe rozwiązania organizacyjne służące ochronie danych, a certyfikacja wg norm sprzyja skutecznemu zarządzaniu w tym obszarze. Ich implementacja nie tylko gwarantuje ochronę danych, ale też stawia firmę w lepszej pozycji negocjacyjnej z globalnymi partnerami.

Oto kilka najważniejszych i najczęściej stosowanych norm i standardów w dziedzinie zarządzania danymi:

1. ISO/IEC 27001 - międzynarodowy standard dotyczący systemów zarządzania bezpieczeństwem informacji (ISMS);
2. NIST Cybersecurity Framework - ramy pracy opracowane przez NIST do poprawy zarządzania cyberbezpieczeństwem w organizacjach;
3. COBIT (Control Objectives for Information and Related Technologies) - ramy pracy dotyczące IT governance i zarządzania, które pomagają organizacjom w zapewnieniu, że technologia informacyjna wspiera i realizuje cele biznesowe;
4. TISAX (Trusted Information Security Assessment Exchange) - standard oceny dla przemysłu motoryzacyjnego, który pomaga znormalizować i usprawnić praktyki dotyczące bezpieczeństwa informacji w całym łańcuchu dostaw.

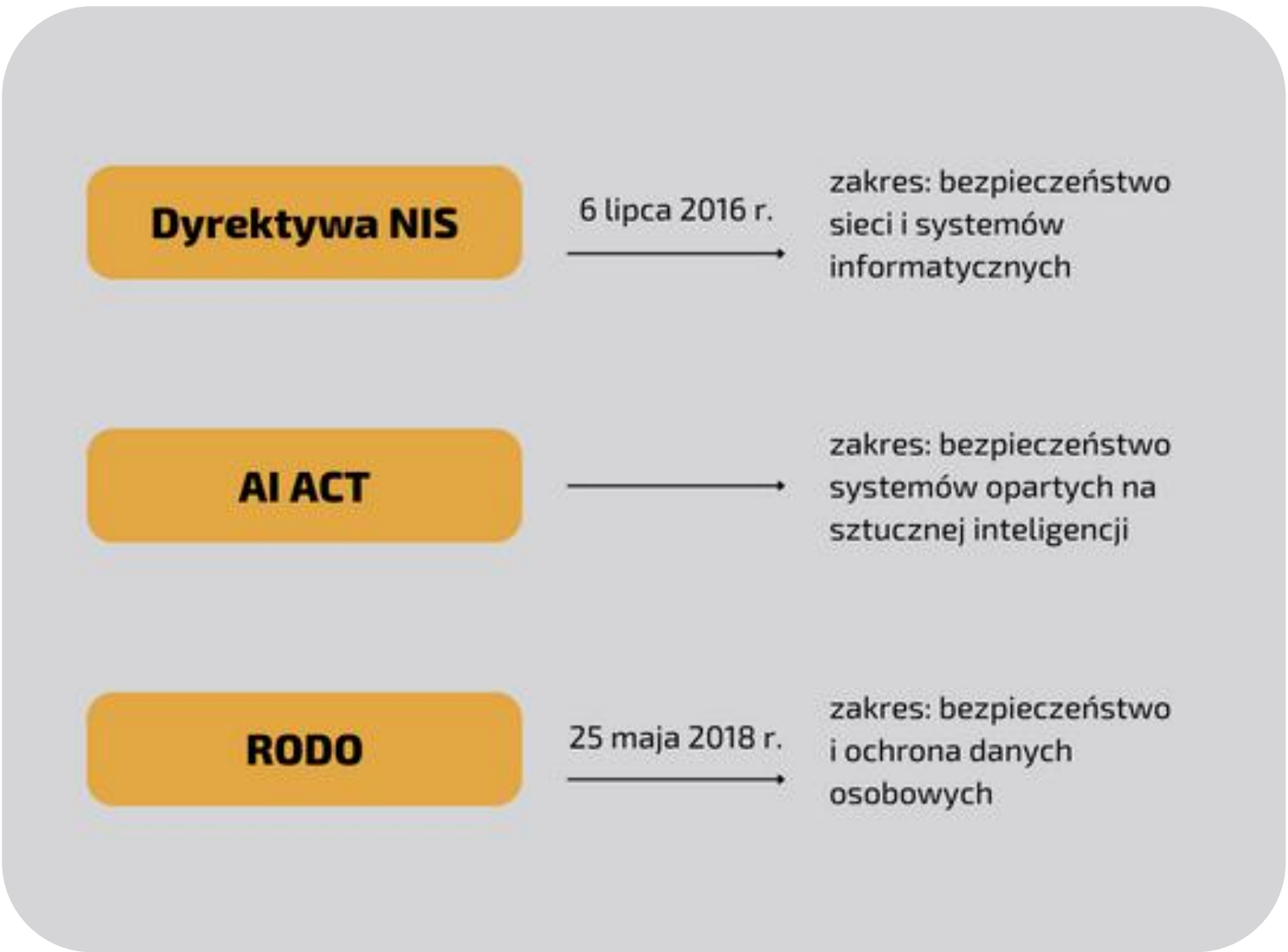
Normy prawa w bezpieczeństwie danych w Unii Europejskiej

Standardy ułatwią usystematyzowanie zasad zarządzania danymi w firmie, nie zapominajmy jednak, iż przedsiębiorcy działają w konkretnym środowisku prawnym, które jest zobowiązaniem przedsiębiorcy, a nie jego wyborem. Zwracam uwagę oczywiście na przepisy prawa z obszaru bezpieczeństwa informacji.

Dyrektywa NIS. W obliczu rosnącej liczby zagrożeń cybernetycznych Unia Europejska wprowadziła Dyrektywę NIS, która skupia się na bezpieczeństwie sieci i systemów informatycznych. Firmy z kluczowych sektorów gospodarki oraz dostawcy usług cyfrowych stają przed nowymi wyzwaniami. Aktualizacja tej dyrektywy – NIS 2 – podnosi poprzeczkę jeszcze wyżej, rozszerzając zakres obowiązków i wskazując nowe podmioty krytyczne.

AI Act. Akt prawa UE w zakresie bezpieczeństwa systemów opartych na sztucznej inteligencji, na który czekamy, a który po ponad kilkumiesięcznych dyskusjach znalazł się na ostatnim etapie procesu legislacyjnego, na etapie konsultacji pomiędzy Parlamentem Europejskim, Radą i Komisją UE [stan na 31 lipca 2023 r.]. Regulacja ma na celu zapewnienie, że systemy sztucznej inteligencji będą nadzorowane przez ludzi, a przy tym bezpieczne, przejrzyste, niedyskryminujące oraz przyjazne dla środowiska.

RODO. Unijną regulację w zakresie ochrony danych osobowych stanowi oczywiście Rozporządzenie o Ochronie Danych Osobowych (RODO). Jest to podstawowy akt prawny w Unii Europejskiej, który wprowadza zasady dotyczące przetwarzania danych osobowych mieszkańców UE.



Przetwarzanie

oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:

- zbieranie,
- utrwalanie,
- organizowanie,
- porządkowanie,
- przechowywanie,
- adaptowanie lub modyfikowanie,
- pobieranie,
- przeglądanie,
- wykorzystywanie,
- ujawnianie poprzez przesłanie,
- rozpowszechnianie lub innego rodzaju udostępnianie,
- dopasowywanie lub łączenie,
- ograniczanie,
- usuwanie lub niszczenie,

a zwłaszcza te, które wykonuje się w systemach informatycznych.

art. 4 pkt 2 RODO

Kluczowe z nich znajdują się w art. 5 RODO, który prezentuje "złote reguły" przetwarzania danych osobowych:

- rzetelność i przejrzystość: dane muszą być przetwarzane w sposób jasny i zrozumiały;
- ograniczenie celu: dane gromadzone są do określonych celów i nie mogą być wykorzystywane w sposób niezgodny;
- minimalizacja danych: zbierane są tylko te dane, które są konieczne;
- prawidłowość: dane muszą być aktualne;
- ograniczenie przechowywania: dane przechowywane są tylko przez niezbędny czas;
- integralność i poufność: dane są chronione;
- odpowiedzialność: podmioty przetwarzające dane muszą udowodnić ich zgodność z powyższymi zasadami.

W praktyce chodzi o to, aby przetwarzać dane w sposób uczciwy, bezpieczny i jedynie w koniecznym zakresie.

Wnioski

W dzisiejszych czasach, kiedy dane osobowe są tak cenne, jak nigdy dotąd, zagrożenia dla prywatności, choć są elementem szeroko pojętego obszaru bezpieczeństwa danych, to muszą stanowić centralny punkt odniesienia w strategiach bezpieczeństwa informacji.

Idee, w jakich powstaje AI Act, to potwierdzają. Zagrożenia dla prywatności to zagrożenia dla biznesu. Organizacje, które traktują ochronę prywatności jako kluczowy element swojej strategii, lepiej chronią prawa jednostek, w ten sposób zabezpieczają się przed konsekwencjami finansowymi, prawnymi i wzmacniają swoją pozycję i reputację na rynku.



Zagrożenia dla prywatności w organizacjach wg raportu IAPP

Współczesne organizacje, niezależnie od swojej skali czy specyfiki działania, stoją przed wyzwaniem zapewnienia odpowiedniej ochrony prywatności. O różnorodności tych zagrożeń mówi raport IAPP.

Od 2015 roku IAPP (International Association of Privacy Professionals) regularnie prezentuje wyniki badania ryzyka związanego z prywatnością. Jest to nieocenione źródło informacji o aktualnych tendencjach i praktykach w dziedzinie ochrony prywatności. Badanie za 2023 rok, przeprowadzone we współpracy z KPMG, dostarcza unikatowego wglądu w najbardziej palące zagrożenia oraz strategię zarządzania nimi.

Najczęstszym ryzykiem związanym z prywatnością zidentyfikowanym przez uczestników badań były trudności w utrzymaniu zgodności z różnymi systemami regulacyjnymi o różnych i/lub zmieniających się wymaganiach.

Analiza metod zarządzania ryzykiem związanym z prywatnością wskazuje, iż:

- prawie 30% organizacji korzysta przy tym tylko z arkuszy kalkulacyjnych;

- tylko 50% organizacji ma ustaloną granicę ryzyka, jaką jest w stanie podjąć w dążeniu do osiągnięcia założonych celów biznesowych;
- 64% organizacji posiada program zarządzania ryzykiem prywatności, który jest w pełni zintegrowany z ogólnym programem zarządzania ryzykiem w przedsiębiorstwie [ISMS];
- 83% organizacji umieszcza informacje o ryzyku, związanym z prywatnością w swoim raporcie rocznym;
- prawie 93% organizacji wskazało, że prywatność jest jednym z 10 najważniejszych ryzyk organizacyjnych, a 36% umieściło ją w pierwszej piątce.

Główne zagrożenia według raportu to:

- naruszenia bezpieczeństwa danych;
- niezgodne z prawem przetwarzanie danych przez podmioty trzecie;
- niewłaściwe wdrożenie ochrony prywatności już na etapie projektowania;
- niewystarczające zarządzanie danymi osobowymi;
- braki w szkoleniach dla pracowników z zakresu ochrony prywatności.

Inne najwyżej oceniane zagrożenia to:

- zrównoważenie wymogów, dotyczących lokalizacji danych z potrzebami biznesowymi UE;
- niezamierzone konsekwencje, które wynikają z niedojrzałości w zarządzaniu zagrożeniami dla prywatności, które pojawiają się w związku z wykorzystaniem sztucznej inteligencji oraz
- zagrożenia dla prywatności, wynikające z wysiłków na rzecz monetyzacji danych.

W mojej opinii edukacja pracowników w zakresie ochrony danych osobowych i prywatności jest absolutnie kluczowa. Dlaczego? Ponieważ w wielu przypadkach to właśnie ludzki błąd stanowi przyczynę naruszeń bezpieczeństwa. Często słyszymy o zaawansowanych atakach cybernetycznych, ale rzeczywistość jest taka, że wiele naruszeń ma miejsce z powodu prostych błędów, takich jak wysyłanie wiadomości e-mail do niewłaściwego odbiorcy czy klikanie w podejrzane linki. Regularne szkolenia dla pracowników zapewniają, że są oni świadomi potencjalnych zagrożeń i wiedzą, jak postępować, aby ich unikać. W erze, w której dane stają się

aktywem dla wielu organizacji, nie możemy pozwolić na ich utratę z powodu braku wiedzy lub zrozumienia.

Osobiście dodałabym zagrożenia, związane z szybkim rozwojem technologii. Przykład: Internet rzeczy. Liczba podłączonych do sieci urządzeń zwiększa się w geometrycznej progresji – mądre zegarki, kamery do monitoringu, inteligentne żarówki czy roboty sprzątające – każde z nich zbiera dane, a co za tym idzie: ekspozycja na potencjalne naruszenia ciągle rośnie. Ponadto zagrożenia związane z atakami typu "phishing" i inne techniki socjotechniczne to nadal poważne wyzwanie. Skupiają się one na najbardziej podatnym elemencie systemu bezpieczeństwa, czyli człowieku.

Nie możemy też nie wspomnieć tutaj o skoku technologicznym w obszarze sztucznej inteligencji. Narzędzia oparte na AI, w tym modele LLM (jak GPT-4, na którym opiera się ten model), umożliwiają organizacjom przetwarzanie ogromnych ilości danych w ekstremalnie krótkim czasie, przewidywanie trendów czy nawet komunikację z klientami. Ale co, jeśli te modele zostaną źle wytrenowane lub wykorzystane w niewłaściwy sposób?

Mogą one prowadzić do nieścisłości, błędów lub, co gorsza, do dyskryminacji lub naruszenia prywatności. Modele takie mogą działać w sposób, który jest trudny do zrozumienia nawet dla ekspertów. Bez odpowiedniego nadzoru, AI może nieświadomie naruszać normy etyczne i regulacje prawne, prowadząc do potencjalnych skandali, które szkodzą reputacji firmy i narażają ją na ryzyko prawne.

” W erze, w której dane stają się najważniejszym aktywem dla wielu organizacji, nie możemy pozwolić na ich utratę z powodu braku wiedzy lub zrozumienia.

Podsumujmy tutaj wnioski z raportu i własne. Żyjemy w erze, w której technologia i dane odgrywają kluczową rolę w funkcjonowaniu większości organizacji. Aby skutecznie zarządzać ryzykiem związanym z prywatnością, organizacje muszą dostrzegać powagę ryzyk dla danych osobowych, inwestować w edukację pracowników i być świadome potencjalnych pułapek związanych z nowoczesnymi technologiami, takimi jak sztuczna inteligencja.



Awers i rewers konsekwencji zagrożeń dla danych osobowych

Konsekwencje zagrożeń w kontekście ich wagi i prawdopodobieństwa zmaterializowania się mają dwojaki charakter. Z jednej strony stanowią wymierne ryzyko dla szeroko pojętych interesów Twojej firmy, ale z drugiej strony to konkretne ryzyka dla praw i wolności osób – Twoich klientów i pracowników.

Obie strony tego medalu są równie istotne i jeśli dostrzeżesz wagę bezpieczeństwa danych osobowych i uwzględnisz szczególny sposób zarządzania nimi zgodnie z RODO, to korzyści z takiego podejścia będą wymierne dla Twoich interesów biznesowych jako przedsiębiorcy.

Typ	Zagrożenia dla firmy [awers]	Zagrożenia dla praw i wolności osób fizycznych [rewers]
Koncentracja na	konsekwencjach zagrożeń dla organizacji	wpływie zagrożeń na prywatność osób fizycznych
Podejście	zarządzanie ryzykiem w przedsiębiorstwie (standardy ISO, NIST, TISAX)	zarządzanie z uwzględnieniem RODO
Cel	wybór i wdrożenie odpowiednich środków technicznych i organizacyjnych, które ograniczają ryzyka	wybór i wdrożenie odpowiednich środków technicznych i organizacyjnych, które ograniczają ryzyka
Konsekwencje / Wpływ(ISO 27557)	konsekwencje bezpośrednio dla przedsiębiorcy: - koszty braku zgodności (grzywny regulacyjne, koszty postępowania sądowego, - koszty działań naprawczych)bezpośrednie koszty biznesowe (utrata przychodów lub wyników spowodowana rezygnacją, lub unikaniem kontaktu z klientem), - uszkodzenie reputacji (uszkodzenie marki, utrata zaufania klientów) - szkody dla wewnętrznej kultury organizacyjnej (wpływ na zdolność organizacji/jednostki w celu osiągnięcia wizji/misji, wpływ na produktywność/morale pracowników wynikający z konfliktów z wewnętrznymi wartościami kulturowymi lub etyką)	konsekwencje dla osoby, której dane są przetwarzane: - utrata godności (w tym zakłopotanie i cierpienie emocjonalne) - dyskryminacja np. rasowa/etniczna, ze względu na płeć, religijna, wiekowa, ze względu na niepełnosprawność czy dyskryminacja ekonomiczna - strata ekonomiczna (może obejmować bezpośrednie straty finansowe w wyniku kradzieży tożsamości lub braku otrzymać wartość godziwą w transakcji) - utrata samostanowienia (utrata autonomii / utrata wolności / uszkodzenie ciała) - utrata zaufania (utrata dobrego imienia i zaufania innych osób)
Specjalne warunki dla wysokiego ryzyka	brak ograniczeń, decyzję podejmuje najwyższe kierownictwo	administrator danych konsultuje się z organem nadzorczym przed przetwarzaniem, jeżeli ocena skutków dla ochrony danych wskazuje, że przetwarzanie skutkowałoby wysokim ryzykiem w przypadku braku środków podjętych przez administratora w celu ograniczenia ryzyka
Metodologia	ISO 31000, COSO ERMISO 27005 (dla ryzyka naruszenia danych)	wytyczne organów nadzorczych (EROD/WP29, ICO, DPC, CNIL, AEPD, APDCAT, PDPC...)

Od czego zacząć zarządzanie ryzykiem dla bezpieczeństwa danych osobowych?

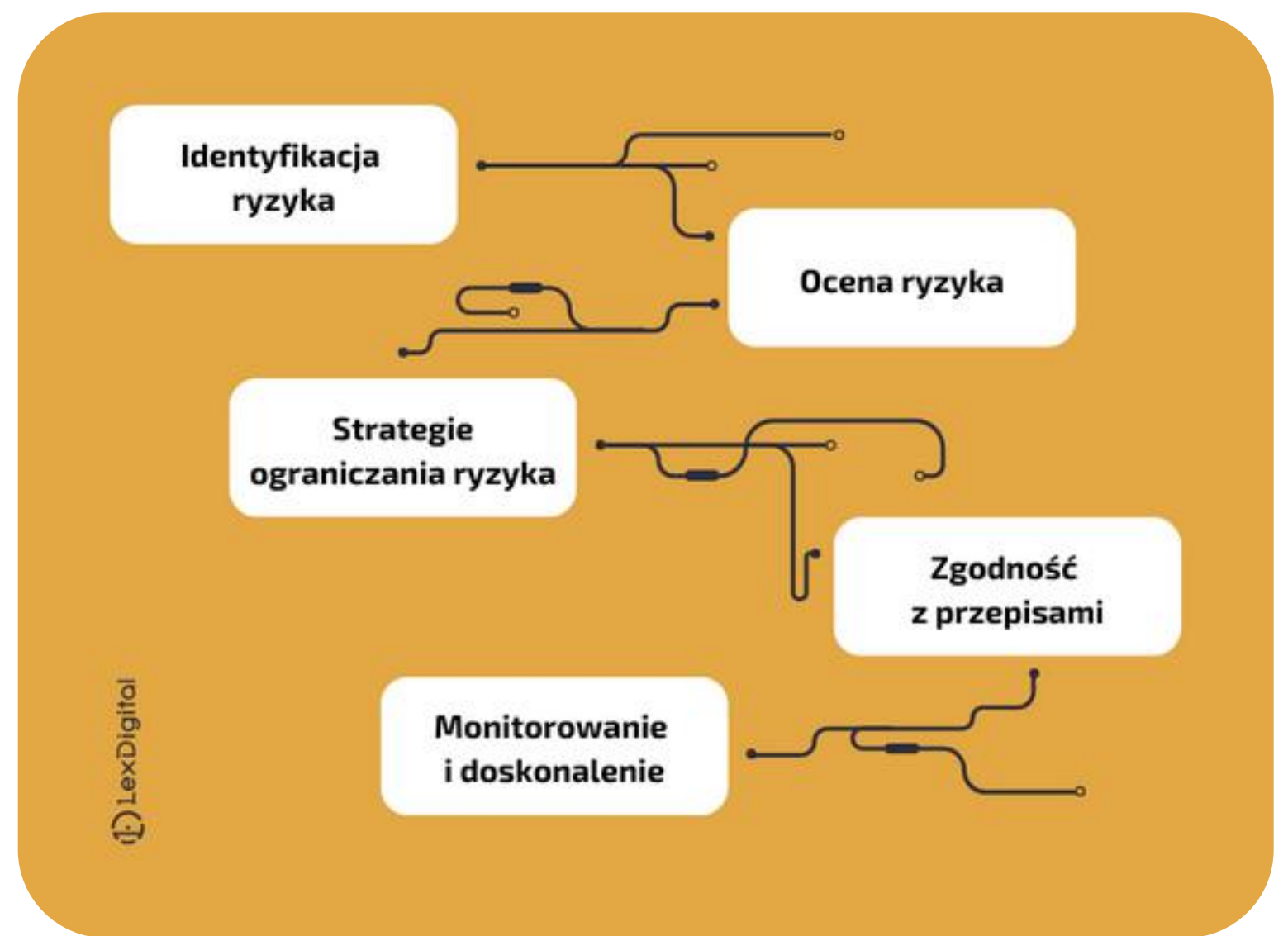
1 krok to identyfikacja ryzyka: pierwszym krokiem w zarządzaniu ryzykiem dla bezpieczeństwa danych osobowych jest identyfikacja różnych zagrożeń, związanych z przetwarzaniem danych osobowych. Obejmuje to również ocenę praktyk gromadzenia, przechowywania i przetwarzania danych w organizacji, a także identyfikację potencjalnych luk w infrastrukturze IT. Zapisy tej identyfikacji znajdują swoje odzwierciedlenie w rejestrze czynności przetwarzania, a gdy organizacja ma status podmiotu przetwarzającego – w rejestrze kategorii czynności przetwarzania opracowanym zgodnie z art. 30 RODO.

2 krok to ocena ryzyka: po zidentyfikowaniu potencjalnych zagrożeń organizacje muszą ocenić wpływ i prawdopodobieństwo ich materializacji. Krok ten obejmuje w przypadku danych osobowych kwantyfikację potencjalnych strat finansowych, prawnych i reputacyjnych, które mogą wynikać z naruszenia danych, ale nie przez pryzmat przedsiębiorstwa – administratora danych, a przez pryzmat osoby, której dane są przetwarzane.

3 krok to strategie ograniczania ryzyka: na podstawie oceny ryzyka organizacje zobowiązane są do opracowania odpowiednich strategii dla złagodzenia zidentyfikowanych zagrożeń. Obejmuje to wdrożenie solidnych środków cyberbezpieczeństwa, protokołów szyfrowania, kontroli dostępu i szkolenia pracowników w zakresie najlepszych praktyk dotyczących prywatności danych. Tutaj środki obniżające ryzyko naruszenia bezpieczeństwa będą zbieżne ze środkami proponowanymi w bezpieczeństwie informacji.

4 krok to zgodność z przepisami: zarządzanie ryzykiem dla bezpieczeństwa danych osobowych musi być dostosowane do przepisów dotyczących ochrony danych. Zgodność z tymi przepisami jest nie tylko wymogiem prawnym, ale także istotnym elementem budowania zaufania klientów.

5 krok to ciągłe monitorowanie i doskonalenie: zagrożenia dla prywatności danych są dynamiczne, a nowe zagrożenia pojawiają się regularnie. Dlatego też skuteczny plan ciągłości działania wymaga



systematycznego monitorowania środków ochrony prywatności danych, regularnych audytów i okresowych przeglądów w celu zapewnienia, że istniejące kontrole pozostają skuteczne i aktualne.

Jakie są najważniejsze elementy wdrażania zarządzania ryzykiem dla prywatności danych?

Mapowanie danych: zrozumienie przepływu danych w organizacji i zidentyfikowanie miejsc, w których przechowywane lub przetwarzane są wrażliwe informacje. Pomaga to w ocenie potencjalnych słabych punktów i wdrożeniu odpowiednich środków kontroli.

Szkolenie pracowników: pracownicy są często najsłabszym ogniwem w ochronie prywatności danych. Regularne szkolenia i programy uświadamiające są niezbędne do edukowania personelu na temat zagrożeń dla prywatności danych i znaczenia bezpiecznych praktyk przetwarzania danych.

Minimalizacja danych: zbieraj i przechowuj tylko te dane, które są niezbędne do prowadzenia działalności. Zmniejszenie ilości wrażliwych danych minimalizuje potencjalny wpływ naruszenia.

Szyfrowanie i anonimizacja: wdrożenie solidnych mechanizmów szyfrowania danych zarówno w spoczynku, jak i w transzycie. Ponadto anonimizacja danych, gdy jest to możliwe, może stanowić dodatkową warstwę ochrony.

Plan reagowania na incydenty: opracowanie kompleksowego planu reagowania na incydenty, który określa kroki, jakie należy podjąć w przypadku

naruszenia danych lub prywatności. Plan ten powinien obejmować role, obowiązki i protokoły komunikacji.

Ochrona danych osobowych ze wsparciem LexDigital

Ponieważ dane stają się coraz bardziej wartościowe, a tym samym podatne na zagrożenia, zarządzanie ryzykiem operacyjnym jest niezbędną praktyką ochrony prywatności danych. Poprzez proaktywną identyfikację, ocenę i ograniczanie ryzyka, związanego z prywatnością danych, zyskujesz zaufanie swoich klientów, przestrzegasz przepisów oraz unikasz kosztownych i szkodliwych naruszeń danych. Chronisz się nie tylko przed karą – chronisz wizerunek swojej organizacji.

Potrzebujesz wsparcia w obszarze ochrony danych osobowych i bezpieczeństwa informacji? Napisz do nas! Dzięki współpracy z zespołem ekspertów LexDigital zyskujesz wsparcie w ramach monitorowania, ulepszania i stosowania najlepszych praktyk w zakresie prywatności danych. Razem z LexDigital możesz pewnie poruszać się po cyfrowym krajobrazie, zapewniając poufność wrażliwych informacji w dynamicznej i stale ewoluującej erze cyfrowej.

” Poprzez proaktywną identyfikację, ocenę i ograniczanie ryzyka, związanego z prywatnością danych, zyskujesz zaufanie swoich klientów, przestrzegasz przepisów oraz unikasz kosztownych i szkodliwych naruszeń danych.

CHCESZ SKORZYSTAĆ Z NASZEJ OFERTY? NIE CZEKAJ!

Odpowiemy na nurtujące Cię pytania, zaplanujemy spotkanie, przygotujemy spersonalizowaną ofertę dopasowaną do potrzeb Twojej organizacji.

E-mail: biuro@lexdigital.pl
Tel.: +48 500 214 942



Aleksander Markiewicz

Compliance – czy jest tak bardzo potrzebne w przedsiębiorstwie i dlaczego? Wchodzimy w szczegóły

Obszar zgodności z przepisami prawa krajowego i międzynarodowego, a także innymi normami postępowania powinien obejmować całość działalności organizacji. Pomaga to nie tylko monitorować i egzekwować regulaminy organizacji czy chronić się przed naruszeniami, ale także jest to sposób na zwiększenie zaufania klientów i partnerów biznesowych do Twojej firmy.

Minimalny zakres obszaru zgodności powinien obejmować obszary, w których działania i zapewnienie zgodności są wymagane przepisami prawa (np. RODO czy AML). W pozostałym zakresie, a więc tam, gdzie zgodność będzie działaniem dobrowolnym organizacji (dobrą praktyką), celem systemu compliance będzie minimalizacja ryzyka wystąpienia zdarzeń negatywnych dla organizacji (np. straty wizerunkowe czy straty finansowe).

W ramach naszej oferty pomagamy w rozwiązaniach compliance w zakresie: HR, e-commerce, ubezpieczenia, BHP, marketing, ochrona konkurencji i konsumenta, AML, sygnaliści. Wsparcie w obszarze compliance, które oferujemy ma szeroki zakres i wszystko zależy od potrzeb Twojej firmy.

Możemy pomóc w przeprowadzeniu audytu zerowego, zająć się bieżącym wsparciem, wspomóc w audycie okresowym, zapewnić Ci wsparcie Compliance Officer'a, czy przeprowadzić szkolenia dla pracowników.

Od czego zacząć i dlaczego w każdej firmie compliance wygląda inaczej?

Każda organizacja do zagadnień zgodności powinna podejść w sposób indywidualny, dlatego trudno jest przygotować jedno rozwiązanie w zakresie zgodności, które będzie uniwersalne i będzie pasowało do każdej organizacji.

Różnorodność organizacji wynika m.in. z rynku, na jakim działają (krajowy lub międzynarodowy), branży (finanse, produkcja, sprzedaż, e-commerce), kultury organizacyjnej czy wielkości organizacji.

Aby zbudować i wdrożyć skuteczny system zgodności konieczne jest uwzględnienie wszystkich zmiennych w danej organizacji, tak aby regulacje

wewnętrzne i narzędzia do ich realizacji były dopasowane do potrzeb i możliwości organizacji.

Przy budowaniu systemu zgodności należy wziąć pod uwagę, jakim przepisom i regulacjom podlega organizacja, co będzie determinowało obowiązek zapewnienia zgodności w tych obszarach.

W zależności od przedmiotu działalności organizacja może podlegać określonym organom nadzorczym – np. podmioty świadczące usługi finansowe będą podlegały kontroli ze strony KNF, a podmioty świadczące usługi telekomunikacyjne podlegają kontroli UKE, natomiast podmioty importujące drewno spoza UE mogą podlegać kontroli ze strony wojewódzkich inspektoratów ochrony środowiska. Biorąc pod uwagę liczbę regulacji oraz tempo zmian w otoczeniu prawnym każda organizacja bez skutecznego systemu narażona jest na brak zgodności.

” Każda organizacja chcąc wdrożyć system zgodności musi w pierwszej kolejności zidentyfikować obszary, w których jest zobowiązana zapewnić zgodność oraz obszary, które mogą generować największe ryzyka dla organizacji

Obszary wewnętrzne i obowiązki

Poza obszarami nadzorowanymi przez organy nadzorcze, w każdej organizacji występują obszary generujące ryzyko, których objęcie systemem zgodności nie jest obowiązkowe z mocy prawa, ale może pozwolić organizacji na znaczne zmniejszenie ryzyka wystąpienia sytuacji niepożądanych. Do takich obszarów należy zaliczyć obszar HR, który obejmuje proces rekrutacji, etap zatrudnienia oraz etap zakończenia stosunku pracy lub stosunku cywilnoprawnego. Najobszerniejszym etapem jest etap zatrudnienia, który obejmuje m.in. badania okresowe, podróże służbowe, realizację praw pracownika, czas pracy – każdy z tych obszarów generuje inne ryzyka.

Każda organizacja chcąc wdrożyć system zgodności musi w pierwszej kolejności zidentyfikować swoje obowiązki, a więc obszary, w których jest zobowiązana zapewnić zgodność oraz obszary, które mogą generować największe ryzyka dla organizacji (np. ryzyko finansowe czy utraty reputacji). Następnie konieczne jest ustalenie

priorytetów działań, mających na celu wdrożenie systemu zgodności. Samo wdrożenie systemu nie ogranicza się tylko do przyjęcia i ogłoszenia polityk i procedur, ale również powinno obejmować cykliczne szkolenia i uświadamianie personelu w zakresie obowiązków związanych z zachowaniem zgodności.

Compliance w krokach. Jakie działania kryją się pod pojęciem zgodności?

Audyt zerowy

Pozwala na weryfikację: jakim przepisom podlega organizacja, jaki jest poziom zgodności, jaka jest świadomość zapewnienia zgodności w organizacji, a także pozwala na identyfikację ryzyk i opracowanie planu wdrożenia systemu zgodności.

Bieżące wsparcie

Polega na bieżącym doradztwie i wdrożeniu rozwiązań, które będą zmierzać do zapewnienia organizacji zgodności. Bieżące wsparcie obejmuje swoim zakresem konsultacje w sprawach wпадkowych, wsparcie w planowaniu systemu zgodności oraz przygotowanie do implementacji nowych obowiązków wynikających z przepisów.

Audyt okresowy

Ten rodzaj audytu ma na celu okresową weryfikację poziomu zgodności, prawidłowości wdrożonych rozwiązań oraz wyznaczenie obszarów do zmiany lub rozwoju. Audyt okresowy skupia się na identyfikacji obszarów wymagających doskonalenia, określeniu skuteczności wcześniejszych wdrożeń oraz opracowania planu naprawczego w wybranych obszarach.

Outsourcing funkcji Compliance Officera

Usługa ta polega na przejęciu funkcji Compliance Officera lub koordynatora obszaru zgodności w organizacji. Osoba wyznaczona z ramienia LexDigital pełni powyższą funkcję poprzez bieżącą koordynację obszaru zgodności, współdziałanie z określonymi komórkami w organizacji oraz wyznaczanie celów długo i krótko terminowych w obszarze zgodności.

Ład korporacyjny

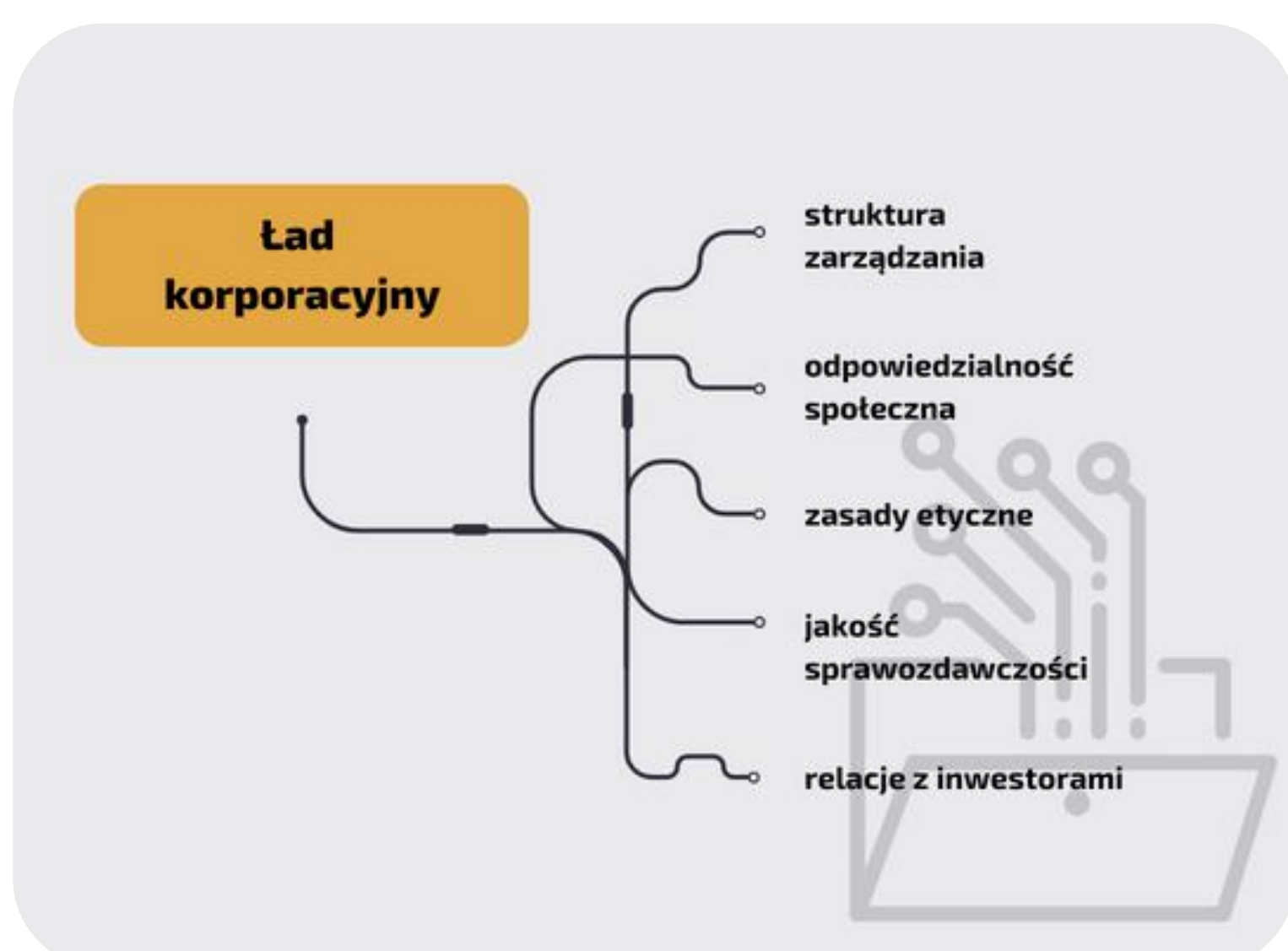
Ład korporacyjny to zbiór zasad i praktyk, które rządzą zachowaniem firm i ich relacjami z interesariuszami.

W ramach ładu korporacyjnego firma musi działać w sposób odpowiedzialny, zgodny z etyką i przestrzegając prawa.

Ład korporacyjny obejmuje wiele aspektów, takich jak:

1. Struktura zarządzania – odpowiednia struktura zarządzania organizacją, zapewnia skuteczne podejmowanie decyzji i kontrolę nad działalnością firmy.
2. Odpowiedzialność społeczna – odpowiedzialność wobec środowiska, społeczności lokalnej i pracowników to nie tylko obowiązek, ale także dobry fundament do budowania relacji z grupą docelową firmy.
3. Zasady etyczne – przestrzeganie wysokich standardów etycznych w swoich działaniach biznesowych zapewnia organizacji bagaż reputacyjny, który może uchronić Twoją firmę i zwiększyć zaufanie klientów i partnerów wobec niej.
4. Jakość sprawozdawczości – publikacja rzetelnych i przejrzystych raportów finansowych oraz informacje dotyczące działań biznesowych są kluczowym elementem w budowaniu zaufania i transparentności w działalności przedsiębiorstwa.
5. Relacje z inwestorami – firma powinna dbać o interesy swoich udziałowców lub akcjonariuszy, ale jednocześnie działać w sposób zgodny z zasadami etycznymi i przepisami prawa.

Wprowadzenie i rozwijanie ładu korporacyjnego pomaga firmom budować zaufanie i lojalność wśród swoich klientów, pracowników, inwestorów i społeczeństwa jako całości. Dzięki temu firma może osiągnąć sukces w dłuższej perspektywie czasowej i przyczynić się do zrównoważonego rozwoju.



Brak wdrożonego ładu korporacyjnego wiąże się z licznymi ryzykami. Są to ryzyka :

1. straty finansowej,
2. utraty reputacji,
3. kar administracyjnych,
4. postępowań sądowych,
5. zdarzeń fraudowych,
6. odpowiedzialności karnej członków zarządu,
7. naruszenia przepisów prawa.

W jakich obszarach organizacji musimy zadbać o zgodność?

HR

Compliance w HR obejmuje wszystkie procesy związane z zatrudnieniem, od procesu rekrutacji, przez okres zatrudnienia, aż do chwili wygaśnięcia stosunku pracy. Rozwiązania w zakresie zachowania zgodności w HR mają na celu minimalizację wystąpienia ryzyk lub ich skutków.

Cel ten osiągamy przez:

- wprowadzenie właściwych procedur i polityk, które określają osoby lub jednostki, odpowiedzialne za dany obszar lub proces;
- budowanie świadomości pracowników;
- określenie zasad onboardingu i offboardingu;
- określenie praw i obowiązków pracowników;
- określenie nakazów i zakazów obowiązujących w organizacji.

BHP

Zgodność w obszarze BHP obejmuje nie tylko rozwiązania wymagane przepisami prawa, ale również rozwiązania, których celem jest minimalizacja ryzyk występujących w tym obszarze. Zapewnienie zgodności w obszarze BHP jest szczególnie istotne w branży produkcyjnej oraz usługowej – zwłaszcza jeśli występują prace szczególnie niebezpieczne lub występują przekroczenia najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych.

Ubezpieczenia

Zgodność w obszarze dystrybucji ubezpieczeń obejmuje nie tylko zgodność z przepisami o dystrybucji ubezpieczeń, a co za tym idzie zgodność w obszarze nadzorowanym przez Urząd Komisji

Nadzoru Finansowego, ale również ze względu na częste świadczenie usług na rzecz konsumentów w obszarze nadzorowanym przez Urząd Ochrony Konkurencji i Konsumenta.

” **Samo wdrożenie systemu nie ogranicza się tylko do przyjęcia i ogłoszenia polityk i procedur, ale również powinno obejmować cykliczne szkolenia i uświadamianie personelu w zakresie obowiązków związanych z zachowaniem zgodności.**

Marketing

Compliance w marketingu to przestrzeganie regulacji prawnych, etycznych i standardów branżowych przez firmy prowadzące działania marketingowe. Obejmuje to przestrzeganie przepisów dotyczących prywatności, ochrony konsumentów, reklamy, konkurencji oraz innych regulacji, które wpływają na działania marketingowe.

W praktyce oznacza to, że firmy muszą działać zgodnie z regulacjami prawnymi, takimi jak RODO, Prawo Telekomunikacyjne czy kodeksami etyki. Muszą także stosować się do standardów branżowych i etycznych, takich jak zasady dotyczące rzetelnego przedstawiania produktów czy zasad antyspamowych.

Współczesny marketing wymaga od firm nie tylko kreatywności i innowacyjności, ale także dbałości o zgodność z przepisami i etyką. Właściwe wdrożenie i przestrzeganie zasad compliance w marketingu pomaga firmom uniknąć negatywnych skutków prawnych i reputacyjnych, zwiększa zaufanie konsumentów i buduje ich lojalność wobec marki.

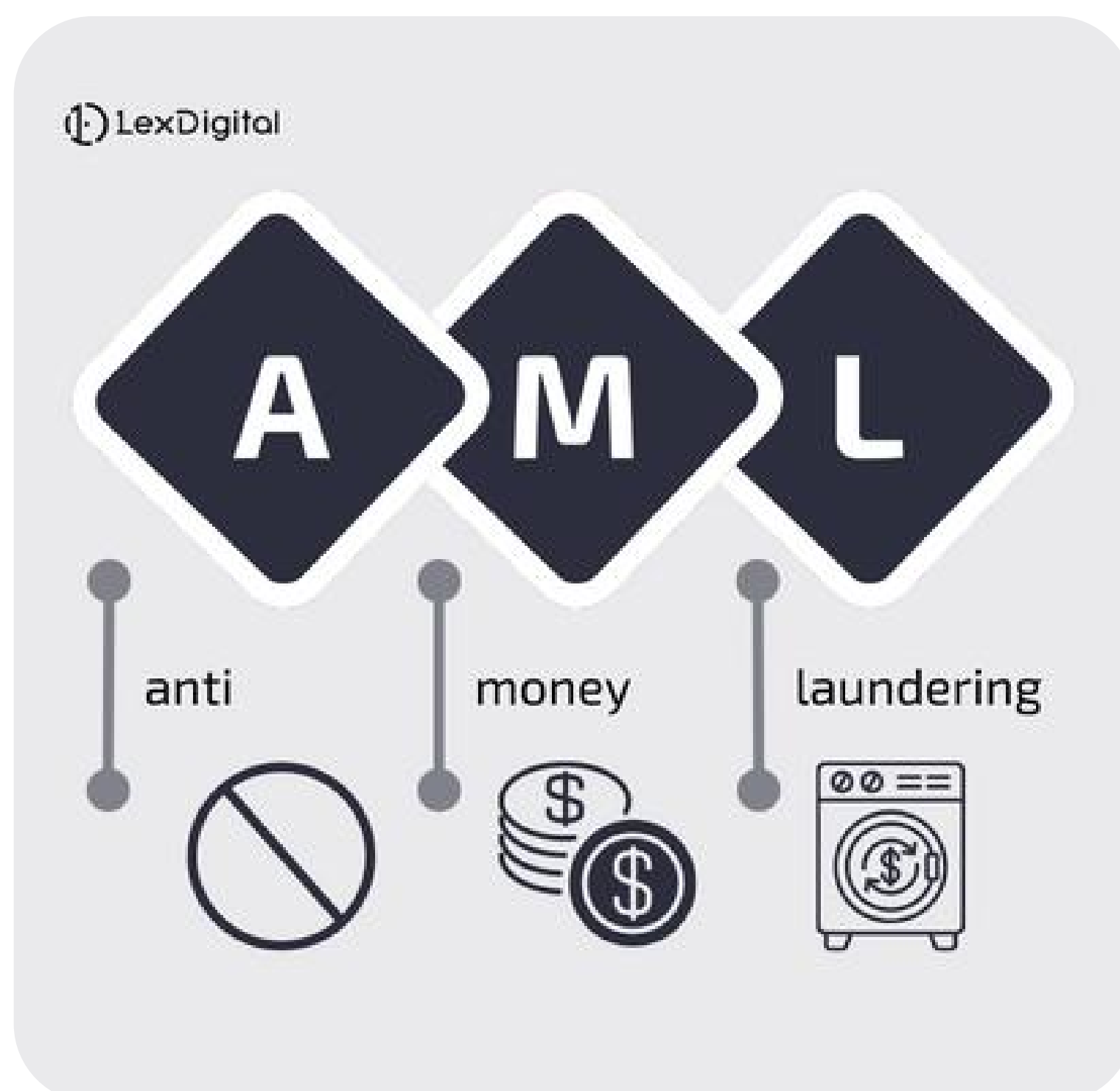
Ochrona konkurencji i konsumentów

Compliance w obszarze ochrony konkurencji i konsumentów to zapewnienie zgodności działań przedsiębiorstw z obowiązującymi przepisami prawa, które dążą do ochrony konsumentów oraz zapobiegania nieuczciwej konkurencji na rynku.

Obejmuje to między innymi:

1. zapewnienie zgodności z przepisami dotyczącymi ochrony konsumentów, takimi jak prawa konsumenta do informacji, prawa do reklamacji, prawa do odstąpienia od umowy i inne;

2. zapobieganie praktykom nieuczciwej konkurencji, takim jak nierzetelna reklama, oszustwa handlowe, sprzedaż produktów niskiej jakości lub zafałszowanie danych produktów;
3. monitorowanie rynku i konkurencji w celu wykrycia i zapobiegania praktykom nieuczciwej konkurencji i ochrony przedsiębiorstw przed naruszeniem prawa antymonopolowego.



AML

AML (Anti-Money Laundering) to kompleksowe podejście, którego głównym celem jest zapobieganie praniu brudnych pieniędzy i finansowaniu terroryzmu. Compliance w obszarze AML to zbiór działań i procedur, mających na celu spełnienie wymagań prawnych, związanych z zapobieganiem praniu pieniędzy oraz finansowaniu terroryzmu. W skład tych działań wchodzi między innymi:

1. weryfikacja tożsamości klienta, w tym weryfikacja źródeł dochodów,
2. raportowanie podejrzanych transakcji organom odpowiedzialnym za zwalczanie prania pieniędzy i finansowanie terroryzmu,
3. prowadzenie szkoleń dla pracowników, w celu uświadomienia im zagrożeń związanych z praniem pieniędzy i finansowaniem terroryzmu,
4. opracowanie wewnętrznych procedur zapobiegania praniu pieniędzy,
5. nadzorowanie procesów finansowych w firmie w celu wychwycenia podejrzanych transakcji,
6. bieżące aktualizowanie procedur związanych z AML zgodnie z obowiązującymi przepisami.

Sygnaliści

Compliance w obszarze systemów whistleblowingowych to zapewnienie i wdrożenie ustawowych i etycznych wymogów dotyczących ochrony sygnalistów, którzy zgłaszają nieprawidłowości w firmie. Taka ochrona zachęca ludzi do ujawniania informacji o naruszeniach prawa i etyki, a także zapewnia im bezpieczeństwo i zapobiega represjom lub innym negatywnym konsekwencjom, wynikającym z ujawnienia takich informacji. Prawidłowo wdrożony system zgłaszania naruszeń to nie tylko realizacja przepisów w tym zakresie, ale również znakomite źródło wiedzy o niedoskonałościach i niezgodnościach występujących w organizacji.

Podsumowanie

Każda organizacja podlega regulacjom prawnym w mniejszym lub większym zakresie, a co za tym idzie – każda organizacja powinna zadbać o zgodność działania z przepisami prawa. Osiągnięcie i utrzymanie zgodności stanowi obecnie duże wyzwanie, co wynika z bardzo dynamicznie rozwijającego i zmieniającego się środowiska prawnego, zarówno na poziomie krajowym, jak i wspólnotowym.



Prasówka

Opublikowano sprawozdanie z działalności PUODO za 2022 rok

25 sierpnia UODO opublikował świeże sprawozdanie z działalności Prezesa UODO w roku 2022. Dokument ma ponad 300 stron i zawiera wiele ciekawych informacji, natomiast nas szczególnie zainteresowały takie kwestie.

Prezes UODO wszczął w 2022 r. z urzędu 34 postępowania w przedmiocie nałożenia administracyjnej kary pieniężnej za brak współpracy z Prezesem UODO i za niezapewnienie mu dostępu do informacji niezbędnych do realizacji jego zadań.

Oznacza to wzrost o 42% w stosunku do poprzedniego okresu sprawozdawczego, w którym tego rodzaju postępowań wszczętych zostało 24.

W 2022 r. Prezes UODO skorzystał z uprawnienia do zastosowania administracyjnej kary pieniężnej w dziewiętnastu sprawach, nakładając na dwadzieścia podmiotów administracyjne kary pieniężne w łącznej kwocie 7 850 861 zł. W porównaniu z rokiem poprzednim oznacza to wzrost ilościowy o dwie kary i blisko 3,5-krotny wzrost wartości nałożonych kar. Dla porównania, w 2021 r. orzeczonych zostało osiemnaście administracyjnych kar pieniężnych na łączną kwotę 2 288 007,50 zł.

W 2022 r. do Urzędu Ochrony Danych Osobowych wpłynęły 12 772 zgłoszenia naruszeń.

Źródło: [Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2022](#)

LexDigital

Najczęściej zgłaszane do UODO oraz typowe naruszenia w 2022 r. to:

- nieprawidłowe zaadresowanie korespondencji zarówno w formie tradycyjnej, jak i elektronicznej;
- udostępnienie danych niewłaściwej osobie;
- nieprawidłowa anonimizacja danych lub niezamierzona ich publikacja;
- zagubienie korespondencji przez operatora pocztowego lub otwarcie korespondencji przed zwróceniem jej do nadawcy;
- nieuprawniony dostęp do baz danych;
- zagubienie, kradzież lub pozostawienie w niezabezpieczonej lokacji dokumentacji papierowej;
- zagubienie lub kradzież nośnika danych;
- wykorzystanie złośliwego oprogramowania ingerującego w poufność;
- integralność lub dostępność danych osobowych.

Źródło: Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2022

Hiszpania tworzy agencję ds. Nadzoru Sztucznej Inteligencji

Hiszpania ogłosiła utworzenie Agencji ds. Nadzoru Sztucznej Inteligencji (AESIA), co jest wydarzeniem bez precedensu w Unii Europejskiej.

“Postęp technologii [AI] w skali globalnej jest niekwestionowany” - czytamy w dekrete królewskim, który ukazał się 22 sierpnia 2023 roku.

Agencja ta będzie pracować nad rozwojem "inkluzywnej, zrównoważonej i skoncentrowanej na obywatelu" sztucznej inteligencji, zgodnie z Krajową Strategią ds. Sztucznej Inteligencji kraju. AESIA będzie funkcjonować w ramach Ministerstwa Spraw Gospodarczych i Transformacji Cyfrowej.

Źródło: [oświadczenie ministerstwa finansów i służby publicznej](#)

” Postęp technologii [AI] w skali globalnej jest niekwestionowany

UODO sprawdzi procedury weryfikacyjne w Ryanair

Urząd Ochrony Danych Osobowych (UODO) postanowił przyrzeć się bliżej, jak linia lotnicza Ryanair zarządza danymi osobowymi podczas procesu weryfikacji podczas lotów. Dzieje się to w odpowiedzi na liczne sygnały od podróżnych dotyczące procedur weryfikacyjnych stosowanych przez tę linię lotniczą. Urząd chce wyjaśnić, czy procesy te są zgodne z przepisami o ochronie danych osobowych i czy nie stanowią zagrożenia dla prywatności pasażerów.

Pasażerowie zgłaszali m.in., że linia lotnicza żąda skanów dowodów osobistych podczas odprawy, a w przypadku odmowy, nakłada opłatę za weryfikację tożsamości w systemie komputerowym. Po analizie skarg i uzupełnieniu braków formalnych, sprawa zostanie przekazana do irlandzkiego organu nadzorczego DPC (Data Protection Commission), ponieważ firma Ryanair ma siedzibę w Irlandii.

Źródło: [UODO Aktualności](#)

Ogromne naruszenie ochrony danych w londyńskiej policji

W przypadku poważnego naruszenia bezpieczeństwa Londyńska policja została postawiona w stan wysokiej gotowości po zhakowaniu szczegółów funkcjonariuszy i personelu, a wszystkie 47 000 pracowników otrzymało ostrzeżenie o potencjalnym ryzyku. Policja Metropolitalna prowadzi dochodzenie w sprawie naruszenia danych, które miało miejsce, gdy uzyskano nieautoryzowany dostęp do systemów jednego z jej dostawców. Choć Policja nie ujawniła dokładnego czasu ani liczby dotkniętych pracowników, zapewniła, że zhakowane dane nie obejmują informacji osobistych, takich jak adresy, numery telefonów czy dane finansowe.

Rick Prior, Wiceprzewodniczący Federacji Policji Metropolitalnej, wyraził zaniepokojenie i podkreślił potencjalne konsekwencje niewłaściwego wykorzystania skompromitowanych informacji.

Naruszenie nastąpiło zaledwie kilka tygodni po tym, jak Służba Policji Irlandii Północnej przyznała,



że nieumyślnie ujawniła dane osobowe całego swojego personelu liczącego 10 000 osób. Ujawniono nazwisko i pierwszą literę imienia zarówno funkcjonariuszy policji, jak i pracowników cywilnych, ich odpowiednie stopnie lub klasyfikacje, miejsca pracy i jednostki, z którymi byli związani.

Źródło: <https://www.bbc.com/>

W Holandii wyciekły dane prawie wszystkich posiadaczy domów

Z powodu wycieku danych w Kadastrze krajowym było możliwe uzyskanie dostępu do danych osobowych właścicieli nieruchomości w Holandii, takich jak ich nazwiska i adresy zamieszkania. Nie wiadomo, czy luka w zabezpieczeniach została wykorzystana.

Oryginalnie dane w Kadestrze były przeznaczone dla komorników i notariuszy. Jednak każdy mógł założyć konto i uzyskać do nich dostęp, bez żadnej weryfikacji. Holenderski Urząd Ochrony Danych (AP) określił tę lukę w zabezpieczeniach jako bardzo poważne zagrożenie. Stwierdził, że "nieautoryzowany dostęp stanowił wielkie niebezpieczeństwo dla zagrożonych dziennikarzy, aktywistów i polityków,

a także każdej osoby, która miała do czynienia z złośliwym lub prześladowującym byłym partnerem". Urząd ten zobowiązał Kadrę do jak najszybszego jej usunięcia.

Stowarzyszenie Właścicieli Nieruchomości (Vereniging Eigen Huis - VEH) zaapelowało do Ministerstwa Spraw Wewnętrznych i Kadastru o pilne utworzenie zespołu kryzysowego w celu ochrony prywatności właścicieli nieruchomości. Według VEH, problem z bezpieczeństwem danych trwa od lat, a niewiele zostało w tej sprawie zrobione.

VEH podkreśla, że już w 2018 roku udowodnili, że każdy mógł uzyskać poufne dane osobowe za pośrednictwem Kadestra. Każdy, kto założył konto firmowe podając fałszywe dane, nie mógł zostać śledzony, jeśli ubiegał się o informacje. VEH podkreśla, że dane osobowe powinny być dostępne tylko dla osób lub organizacji, które mają "uzasadniony interes". Określone grupy zawodowe, takie jak notariusze, którzy codziennie pracują z tymi danymi i są ściśle nadzorowani, mogą być wyjątkiem od tej reguły. VEH twierdzi, że taka praktyka już obowiązuje w Niemczech.

Źródło: <https://www.rtlnieuws.nl/nieuws/>



Polska

Data: 2023-06-21

Wysokość kary: 33 012,00 zł

H. Sp. z o.o. z siedzibą w W. udostępniła dane osobowe Skarżącego na rzecz podmiotu trzeciego bez podstawy prawnej. Spółka była wielokrotnie wzywana do udzielenia wyjaśnień, nie zareagowała również na fakt wszczęcia postępowania. PUODO nałożył na spółkę administracyjną karę pieniężną za niezapewnienie dostępu do informacji niezbędnych do realizacji jego zadań.

Decyzja PUODO: <https://www.uodo.gov.pl/decyzje/DOKE.561.1.2023>

Data: 2023-06-02

Wysokość kary: 18 864,00 zł

W sprawie udostępniono dane osobowe skarżącego (nr telefonu) podmiotom nieuprawnionym. T. Sp. z o.o. z siedzibą w K. była wielokrotnie wzywana do złożenia wyjaśnień i została pouczone o konsekwencji ich nieudzielenia. Prezes UODO nałożył na spółkę administracyjną karę pieniężną za brak współpracy w ramach wykonywania przez PUODO swoich zadań oraz za niezapewnienie dostępu do informacji.

Decyzja PUODO: <https://www.uodo.gov.pl/decyzje/DKE.561.38.2022>

Świat

Łotewski Urząd Ochrony Danych nałożył karę na firmę za brak udostępnienia dostępu do danych i informacji niezbędnych do przeprowadzenia dochodzenia *ex officio*. Jednak kara została obniżona do 1000 euro z powodu wysokiego ryzyka niewypłacalności firmy. Dochodzenie było prowadzone wspólnie przez Łotewski Urząd Ochrony

Danych, we współpracy z estońskim i litewskim odpowiednikiem.

Wątpliwości dotyczyły legalności działań przetwarzania podejmowanych przez firmę - administratora - w ramach aplikacji mobilnej niezbędnej do korzystania z usług wynajmu samochodów. Urząd Ochrony Danych przeprowadził audyty ochrony danych i zażądał dostępu do danych osobowych i innych informacji niezbędnych do wypełnienia swoich zadań zgodnie z artykułem 58 ust. 1 lit. b i e RODO. Administrator był "nieosiągalny" i nie podporządkował się instrukcjom Urzędu Ochrony Danych. Urząd formalnie wszczął procedurę sankcjonowania administratora.

Źródło: <https://www.dvi.gov.lv/lv/media/2412/download?attachment>

Włoski Urząd Ochrony Danych nałożył karę na lokalny organ zdrowia za wyświetlenie imienia i nazwiska skarżącego w reklamie. Urząd stwierdził naruszenia przepisów artykułów 5(1)(a)(c) (f), 9, 25(1)(2) i nałożył karę w wysokości 25 000 euro zgodnie z artykułem 83. Tablica reklamowa przedstawiała miejsce udzielania pierwszej pomocy, a na widocznym karcie opieki pierwszej pomocy znajdowało się imię i nazwisko osoby, wraz z nazwą jej dostawcy opieki zdrowotnej. Co więcej, reklama umieszczona była przy głównym wejściu do izby przyjęć włoskiego szpitala i była dostępna dla publiczności.

Źródło: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9917728>

Włoski Urząd Ochrony Danych ukarał firmę Cooperjob S.p.A karą w wysokości 20 000 euro za brak spełnienia żądania usunięcia danych osobowych. Żądanie to nie zostało spełnione w terminie i dopiero po 86 dni po pierwotnym żądaniu osoby, której dane dotyczyły i interwencji Urzędu Ochrony Danych doszło do jego wykonania. Urząd Ochrony Danych stwierdził naruszenia przepisów artykułów 12(3) i 17.

Źródło: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9917820>

Cypryjski Urząd Ochrony Danych nałożył karę w wysokości 7 000 euro na lokalną gazetę za naruszenie artykułu 5(1)(c) RODO i artykułu 6 RODO. Gazeta opublikowała imiona i fotografie policjantów na służbie.

W dniu 17 czerwca 2018 roku lokalna gazeta "Politis" (zwana dalej administratorem) opublikowała imiona i fotografie policjantów pełniących służbę na lotnisku w Larnace w artykule zatytułowanym "Awantura policji z 70-letnią turecko-cypryjską kobietą". Skarga została złożona do Cypryjskiego Urzędu Ochrony Danych, a w dniu 14 sierpnia 2018 roku Urząd Ochrony Danych nałożył karę w wysokości 10 000 euro, uzasadniając to naruszeniem artykułu 5(1)(c), artykułu 6 i artykułu 14 RODO.

Ta decyzja została zaskarżona do Cypryjskiego Sądu Apelacyjnego i unieważniona. W międzyczasie artykuł został usunięty z archiwów online gazety. W dniu 14 marca 2022 roku Sąd podjął decyzję o ponownym rozpatrzeniu sprawy przez Urząd Ochrony Danych.

Źródło: [decyzja cypryjskiego organu](#)

14 lipca Norweski Urząd Ochrony Danych (Datatilsynet) nałożył karę na firmę Meta z powodu naruszenia zakazu stosowania marketingu opartego

na zachowaniach na platformach Facebook i Instagram. Jednak Meta złożyła wniosek do sądu w Oslo o czasowe zawieszenie tego zakazu.

Meta nie przestrzega zakazu norweskiego organu ochrony danych, dotyczącego targetowania w mediach społecznościowych, a wyświetlanie reklam wiąże się z inwazyjnym monitorowaniem użytkowników. Zgodnie z decyzją Datatilsynet reklamy behawioralne muszą zostać wstrzymane do czasu znalezienia przez Metę legalnego sposobu na prowadzenie takiego rodzaju marketingu.

W związku z tym, 7 sierpnia Datatilsynet nałożył karę finansową w wysokości miliona koron norweskich za każdy dzień nielegalnej działalności, począwszy od 14 sierpnia.

Meta zwróciła się jednak do sądu w Oslo o czasowe zawieszenie decyzji Datatilsynet. Jeśli sąd przyzna czasowe zawieszenie, Meta nie będzie musiała przestrzegać zakazu Datatilsynet do czasu pełnej rozprawy sądowej.

Tobias Judin, szef międzynarodowego działu Datatilsynet, twierdzi, że warunki na nałożenie czasowego zakazu nie zostały spełnione. Stąd Meta powinna, przestrzegać decyzji organu. Każdy dzień, w którym Meta nie dostosowuje się do naszych zaleceń, oznacza naruszenie prywatności norweskich użytkowników Facebooka i Instagrama - stwierdził.

Źródło: [Datatilsynet](#)

Newsletter RODO

Sierpień 2023 nr 1/2023

Dziękujemy za przeczytanie Naszego Newslettera!

Masz pytania?

[SKONTAKTUJ SIĘ Z NAMI](#)