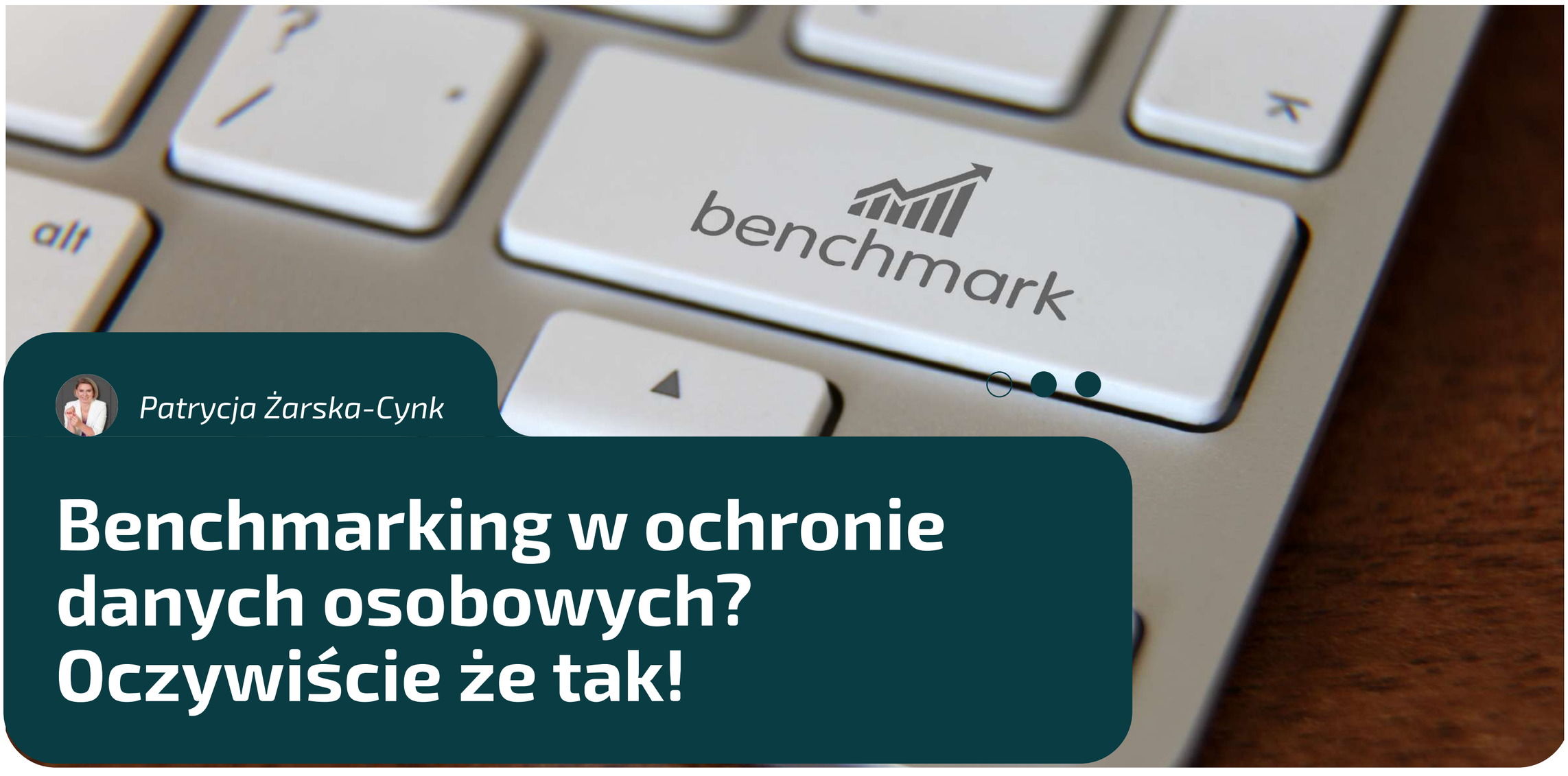
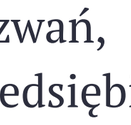
Ryzyko pod kontrolą: jaką strategię zarządzania ryzykiem wybrać?

W TYM WYDANIU:

LexDigital

www.lexdigital.pl





Patrycja Żarska-Cynk

Benchmarking w ochronie danych osobowych? Oczywiście że tak!

Przestrzeganie RODO nie musi być skomplikowane. Oczywiście kluczowe jest mapowanie prowadzonej działalności przez pryzmat danych osobowych, z jakich przy tym korzystasz. Już to bywa trudnym zadaniem, szczególnie gdy masz świadomość wyzwań, jakie stawia RODO przed Tobą jako przedsiębiorcą — administratorem danych osobowych.

Analiza i ewidencja czynności przetwarzania danych, ocena ryzyka, wdrożenie odpowiednich środków ochronnych, ich regularna aktualizacja oraz odpowiednia dokumentacja. Masz świadomość, że te działania nie tylko zapewniają zgodność z prawem, ale także budują zaufanie klientów i partnerów biznesowych do Twojej firmy.

Wiem, że masz, bo subskrybujesz nasz Newsletter!

Proponuję Ci w tym artykule praktyczne podejście oparte na metodzie benchmarkingu. Czym jest benchmarking? To analiza porównawcza stosowana w zarządzaniu przedsiębiorstwem. Benchmarking nie jest zwykłym naśladownictwem, nie polega na podpatrywaniu sposobu pracy innych, aby postępować tak samo. To podpatrywanie jak inni opiekują podobne do Twoich problemy skutecznie, a następnie wykorzystanie tych inspiracji we własnym przedsiębiorstwie.

Jak okazuje się, benchmarking możliwy jest też na gruncie stosowania RODO. Choćby poprzez analizę decyzji organów i zawartych w nich wniosków w poszukiwaniu dobrych praktyk dla zidentyfikowanych słabych stron Twojej firmy.

Proponuję skupić się nie na wysokości kar o jakich przeczytasz w mediach, czy na stronie organów ochrony danych, a na wnioskach płynących z opisanych w decyzjach stanu faktycznego oraz uzasadnienia stanowiska podjętego przez te organy.

Insider — ryzyko dla przetwarzania danych osobowych

Insider w kontekście ochrony danych osobowych to osoba mająca dostęp do wrażliwych lub poufnych danych w ramach organizacji, takiej jak firma czy instytucja. Taka osoba, jest dla ciebie ryzykiem, bo może wykorzystać przyznany jej dostęp do Twoich zasobów, w sposób złośliwy lub niezamierzony, w taki sposób, że będzie mieć negatywny wpływ na firmę. Taka osoba może być pracownikiem, kontraktorem, partnerem biznesowym, czy nawet klientem, który z różnych powodów uzyskała dostęp do danych osobowych przechowywanych przez Twoją firmę jako administratora danych.

Z perspektywy przestrzegania ochrony danych osobowych, insider stanowi zarówno zasób, jak i potencjalne zagrożenie. Jako zasób, insiderzy często posiadają cenne umiejętności i wiedzę niezbędną do

efektywnego zarządzania danymi. Jednakże, ze względu na swoją pozycję i dostęp, mogą również stanowić ryzyko naruszenia bezpieczeństwa danych, zarówno nieumyślnego, jak i celowego.

Insiderzy mogą więc odgrywać kluczową rolę w ochronie danych osobowych, ale jednocześnie wymagają szczególnej uwagi ze strony administratora danych w kontekście zarządzania ryzykiem i bezpieczeństwem informacji.

Nie darmo mamy powiedzenie — “tylko ten, co nic nie robi, nie popełnia błędów”, nic dziwnego więc, że czasami dochodzi do naruszenia danych osobowych z powodu błędów ludzkich, mimo starań i zaangażowania administratora danych.

Co robią Organy Ochrony Danych, gdy podejmą kontrolę w związku z naruszeniem ochrony danych osobowych zainicjowanego przez błąd ludzi? W pierwszej kolejności badają środki techniczne i organizacyjne już wdrożone z intencją zapobiegania możliwości wystąpienia błędu ludzkiego. Gdy okaże się, że w ocenie Organu nasze środki ochrony są bezskuteczne, to Organ bada dalej działania podjęte tuż po zdarzeniu, by ograniczyć negatywne efekty.

Na koniec w wystąpieniu pokontrolnym, w decyzji Organ wskazuje pewne dodatkowe rozwiązania adekwatne jego zdaniem, by ograniczyć tego typu zdarzenia w przyszłości.

Dlatego warto samodzielnie wyciągać wnioski dla swojej organizacji z takich decyzji, traktując je, póki to nie nasze zdarzenia, jak dobre praktyki i istotne rekomendacje. Porada “ucz się na błędach innych” jak widać, ma również swoje miejsce w ochornie danych osobowych.

Środki organizacyjne i techniczne podejmowane wobec Insidera

Administrator danych osobowych ma obowiązek zapewnienia odpowiedniego poziomu ochrony danych już na etapie organizacji pracy. Oczywiście obejmuje to zarządzanie ryzykiem związanym z insiderami. W mojej opinii ten aspekt jest kluczowy.

Zasadniczo, co również wynika z wniosków pokontrolnych, z jakimi miałam przyjemność się zapoznać, **skupiamy się na początek na podstawowych środkach organizacyjnych, do których zaliczamy:**

2. weryfikację i kontrolę dostępu - upewnienie się, że tylko upoważnione osoby mają dostęp do danych osobowych, a ich poziom dostępu jest adekwatny do ich roli i potrzeb;
3. szkolenia i świadomość - regularne szkolenia dotyczące bezpieczeństwa i ochrony danych dla pracowników, aby zwiększyć ich świadomość zagrożeń i nauczyć odpowiednich praktyk;
4. monitoring i audyt - stałe monitorowanie działalności insiderów np. nadzór przełożonych, tak aby wykrywać i reagować na wszelkie nieprawidłowości, które mogą wskazywać na naruszenie ochrony danych;
5. polityki i procedury - wdrożenie jasnych zasad i procedur dotyczących przetwarzania i ochrony danych osobowych, które są zrozumiałe i przestrzegane przez wszystkich insiderów;
6. zarządzanie ryzykiem i reagowanie na incydenty - opracowanie planów zarządzania ryzykiem oraz procedur reagowania na incydenty związane z naruszeniem danych, w tym potencjalne naruszenia spowodowane przez insiderów.

Wśród technicznych rozwiązań królują:

1. szyfrowanie danych - zabezpiecza dane, sprawiając, że bez odpowiedniego klucza są one nieczytelne;

2. regularne tworzenie kopii zapasowych - zapewnia, że w przypadku utraty danych, istnieje ich aktualna kopia;
3. kontrola dostępu - ograniczenie dostępu do danych tylko dla upoważnionych osób.

Oto kilka przykładów konkretnych zdarzeń, które w każdej firmie mogą mieć miejsce oraz wnioski z nich wynikające zawarte w decyzjach Organów Ochrony Danych.

Przykład 1. Wysyłanie masowych wiadomości e-mail, w których wszyscy odbiorcy byli podani w polu “Do” lub “DW”.

W decyzjach Organów Ochrony Danych [EDPBI:CY:OSS:D:2021:182;EDPBI:FR:OSS:D:2021:169] uznano to zdarzenie za naruszenie obowiązków administratora danych w zakresie bezpieczeństwa danych. Skala zdarzenia oczywiście miała znaczenie. Organ stwierdził brak odpowiednich środków technicznych i organizacyjnych w celu zapobiegania takim naruszeniom.

Przykład 2. Przypadkowe ujawnienie danych osobowych jednego klienta innemu klientowi. Tego dotyczyła decyzja [EDPBI:CZ:OSS:D:2019:44].

Pojawiły się tutaj jednak okoliczności łagodzące, wydawać by się mogło nie oczywiste —administrator danych przyjął obowiązkową wewnętrzną procedurę zgłaszania i powiadamiania o naruszeniach ochrony danych osobowych. Ta wewnętrzna procedura obejmowała poszczególne kroki, które należy podjąć po uzyskaniu informacji o naruszeniu, takie jak obsługa incydentu, udokumentowanie incydentu i podjęcie środków naprawczych. Procedura ta obejmowała również metodę przeprowadzania oceny ryzyka i powiadamiania o naruszeniu.

Przykład 3. W kolejnej decyzji [EDPBI:IS:OSS:D:2021:216] Organ Ochrony Danych zwrócił szczególną uwagę, na brak wystarczających testów rozwiązań już wdrożonych przez Administratora w celu zwiększenia bezpieczeństwa danych osobowych w systemie. Okazało się, iż przyjęty mechanizm dopuszczał luki w zabezpieczeniach, które zdaniem Organu doprowadziły do naruszenia danych osobowych.

Przykład 4. Administrator danych, po naruszeniu w postaci ujawnienia adresów e-mail kandydatów do pracy wszystkim odbiorcom wiadomości e-mail, zaproponował jako środek naprawczy, by pracownicy chcąc wysłać e-mail do szerszego grona odbiorców [więcej niż 3 osoby] pytali w pierwszej kolejności o zgodę swojego przełożonego i inspektora ochrony danych [!]. Administrator danych zasugerował również, że pracownik, który popełnił błąd, zostanie poddany rozmowie dyscyplinarnej i będzie musiał przejść dalsze szkolenie. Organ nie uznał jednak tych środków za odpowiednie do spełnienia wymogów art. 32 RODO i zażądał od administratora danych wdrożenia dodatkowych środków technicznych, aby zapobiec wystąpieniu takiego incydentu w przyszłości. Konkretnie, wprowadzenie komunikatu ostrzegawczego wyraźnie wyświetlanego za każdym razem, gdy wiadomość e-mail jest wysyłana do odbiorców spoza organizacji oraz aby wyłączyć pole "cc" lub ograniczyć liczbę adresów e-mail, które to pole może zawierać. Ponadto Organ wymagał, aby za każdym razem, gdy ma zostać wysłana masowa wiadomość e-mail, na ekranie nadawcy pojawiał się komunikat informacyjny w sposób, którego nie można przegapić, a najlepiej uniemożliwiający użytkownikowi wysłanie wiadomości e-mail, chyba że zostanie podjęte pozytywne działanie. Organ wymagał również od firmy skonfigurowania reguły opóźniającej dostarczanie wszelkich wiadomości e-mail [EDPBI:CY:OSS:D:2021:182].

Przykład 5. W kilku przypadkach zaoferowanie przez administratora danych szkolenia z ochrony danych osobowych okazały się wystarczającym środkiem bezpieczeństwa. Organ Ochrony Danych uznał ten środek za istotny gdy naruszenia spowodował błąd ludzki. [EDPBI:DEBE:OSS:D:2020:103;EDPBI:DEBE:OSS:D:2021:197].

Przykład 6. W przypadku błędnej konfiguracji środowiska programistycznego przez pracownika, Organ uznał natychmiastowe unieważnienie tzw. tokena za wystarczający środek bezpieczeństwa [EDPBI:DEBE:OSS:D:2020:103].

Przykład 7. Zaszyfrowana kopia zapasowa bazy danych stała się publicznie dostępna z powodu błędu ludzkiego, Organ uznał środki łagodzące podjęte przez administratora danych za wystarczające. Środki te obejmowały faktyczne usunięcie zagrożonej kopii zapasowej, zablokowanie przechowywania danych, których to dotyczyło, dostarczenie pracownikom pisemnych informacji na temat niezbędnych środków ostrożności przy obchodzeniu się z danymi osobowymi oraz zmianę wszystkich haseł i kodów dostępu do własnych systemów firmy i zintegrowanych systemów stron trzecich. [EDPBI:DEBE:OSS:D:2021:187].

Przykład 8. W następstwie naruszenia danych osobowych, dotyczących klienta, administrator danych zablokował zagrożone konto klienta, zmienił dane, do których uzyskano dostęp, zorganizował szkolenie w zakresie ochrony danych dla pracowników, a inspektor ochrony danych przedsiębiorstwa przeprowadził audyt ochrony danych. Organ uznał te środki za wystarczające [EDPBI:DEBE:OSS:D:2021:197].

Przykład 9. W kilku przypadkach, w których niekrytyczne dane osobowe (często imiona i nazwiska, adresy e-mail lub numery telefonów) stały się publicznie dostępne, Organ stwierdził, że szybkie usunięcie wadliwego kodu lub usunięcie danych przez administratora danych było wystarczającym środkiem. [EDPBI:DEBE:OSS:D:2021:293,EDPBI:DEBE:OSS:D:2021:222,EDPBI:DEBE:OSS:D:2022:349].

Wnioski dla administratora danych

Chciałam zwrócić Ci uwagę w ramach misji podnoszenia Twoich kompetencji w obszarze ochrony danych osobowych, że możesz oczywiście samodzielnie — jako właściciel firmy, lub pracownik na stanowisku zarządczym, zajmować się aspektem

Istotne jest to, że prawo oraz inne regulacje i orzecznictwo dotyczące ochrony danych osobowych to ogromny zasób informacji — oczywiście dostępny w dobie cyfrowej transformacji i narzędzi opartych o generatywną AI, na wyciągnięcie ręki. Czy jednak śledzenie tych zmian samodzielnie nie będzie czasochłonne i skomplikowane?

Zaufaj doświadczonym doradcom, którzy w ramach swojej pracy monitorują informacje prawne oraz decyzje czy rekomendacje organów regulacyjnych. Taki ekspert nie tylko dostarczy tych informacji, które adekwatne są do profilu Twojej działalności, ale również pozwoli Tobie skupić się na głównych aspektach prowadzenia biznesu.

W końcu "co dwie głowy to nie jedna". To już finalne przysłowie, które podkreśla wartość współpracy i efektywności wynikającej z dzielenia się obowiązkami i wspólnego dążenia do celu. W kontekście pracy zespołowej oznacza to, że pracując razem, możemy osiągnąć więcej, niż działając indywidualnie. Popracujemy razem?

Olga Ograbisz

Zarządzanie ryzykiem jako element systemu zarządzania bezpieczeństwem informacji

System bezpieczeństwa informacji zbudowany jest z polityk, procedur, wytycznych, zasobów (kadrowych, finansowych, technicznych) oraz działań, które wspólnie zarządzane przyczyniają się do zapewnienia wysokiego poziomu ochrony aktywów informacyjnych organizacji. Determinantą skuteczności wdrożenia i doskonalenia bezpieczeństwa informacji jest zasada podejścia opartego na ryzyku. Szacowanie ryzyka powinno być bowiem podstawą do wyboru właściwych zabezpieczeń, adekwatnych do podatności danego zasobu i całego kontekstu organizacji. Zabezpieczenia te powinny być następnie odzwierciedlone w tzw. Deklaracji stosowania zabezpieczeń zbudowanej zgodnie ze schematem Załącznika A do normy PN-EN ISO/IEC 27001:2022. Zarządzanie przez ryzyko jako proces ciągły pozwala na racjonalne podejmowanie decyzji związanych z zapewnieniem bezpieczeństwa informacji i efektywną alokację środków, którymi dysponuje w danym momencie organizacja.

Zarządzanie ryzykiem – wymagania normatywne

Ocena ryzyka w bezpieczeństwie informacji to proces identyfikowania, rozwiązywania i zapobiegania problemom bezpieczeństwa. Ocena często opiera się na aktywach, a ryzyko ocenia się w odniesieniu do posiadanych zasobów informacyjnych. Ocena prowadzona jest w całej organizacji. Co więcej, ISO 27001 wyraźnie wymaga, aby proces zarządzania ryzykiem był stosowany do przeglądu i potwierdzania kontroli bezpieczeństwa w świetle obowiązków prawnych i umownych.

Wymagania w zakresie zarządzania ryzykiem wprowadzają rozdziały 6 i 8 oraz pośrednio 9.3.1.2 PN-EN ISO/IEC 27001:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – System zarządzania bezpieczeństwem informacji. WW. punkty nie tylko wskazują na potrzebę identyfikowania ryzyka, ale co ważniejsze na postępowanie z ryzykiem, czyli na działania, jakie organizacja podejmuje wobec zdefiniowanych ryzyk czy też szans.

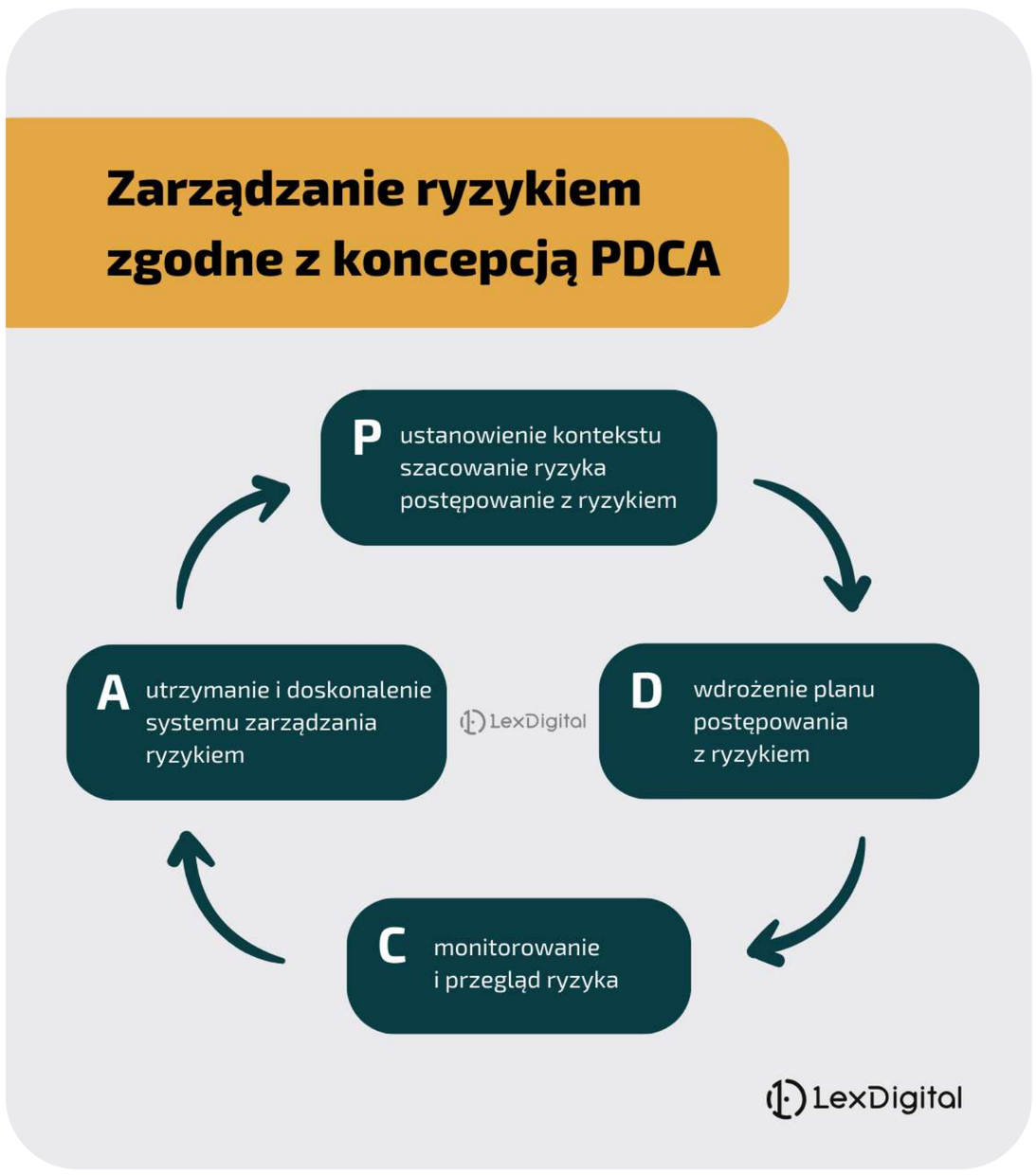
Zarządzanie ryzykiem w bezpieczeństwie informacji

Ryzyko przez normy z serii ISO definiowane jest jako wpływ niepewności na cele, przy czym następstwem niepewności jest odchylenie od oczekiwań zarówno to pozytywne, jak i negatywne. Rozwijając powyższe — pod pojęciem ryzyka rozumie

się prawdopodobieństwo wystąpienia zdarzenia, które będzie miało określony wpływ (skutki) na realizację założonych celów. Rolą podejścia opartego na ryzyku (inaczej zarządzania przez ryzyko) jest dostarczenie informacji o potencjalnych zdarzeniach, które mogą oddziaływać na organizację, jej proces czy też zasób, i podejmowanie na tej podstawie działań jeszcze przed zmaterializowaniem się ryzyka. Daje to organizacji pewny rozsądny poziom pewności, pozwalający na skuteczniejsze zarządzanie danym obszarem działalności, co z kolei przekłada się na finanse organizacji, osiągane cele czy zachowanie bezpieczeństwa aktywów informacyjnych.

Żaden ze standardów ISO nie mówi wprost, w jaki sposób zarządzanie ryzykiem ma się odbywać, w jaki sposób je identyfikować i mierzyć. Podkreśla się natomiast, że metody szacowania ryzyka i postępowania z ryzykiem, powinny być dostosowane do organizacji („szyte na miarę"), a ich wybór powinien uwzględniać estymację kosztów i korzyści, wymagania prawne czy ten inne priorytety i zmienne właściwe dla danej organizacji. Powinny one zapewniać również możliwość porównywania wyników w czasie.

Zaleca się, aby proces zarządzania ryzykiem zgodny z ISO 27001 składał się z ośmiu elementów, które mogą odbywać się zgodnie z zasadą PDCA (Plan Do Check Act) (ilustracja poniżej).



Etapy procesu zarządzania ryzykiem w bezpieczeństwie informacji

Zarządzanie ryzykiem bezpieczeństwa informacji to systemowe działanie polegające na szacowaniu ryzyka (identyfikowanie ryzyka, jego analiza i ocena) oraz podejmowaniu działań na podstawie stwierdzonego ryzyka w taki sposób, aby miało to wartość dodaną dla realizacji celów biznesowych. Jego istotą jest także podejmowanie świadomych i odpowiedzialnych decyzji dotyczących ryzyk.

1. USTANOWIENIE KONTEKSTU

Ustanowienie kontekstu jest pierwszym etapem zarządzania ryzykiem. Jest to moment, w którym organizacja powinna określić i zrozumieć czynniki zewnętrzne i wewnętrzne wpływające na jej funkcjonowanie, cele oraz sposoby ich realizacji. Na kontekst zewnętrzny składają się w szczególności czynniki kulturowe, społeczne, polityczne, ekonomiczne, technologiczne czy finansowe. Są to także relacje, jakie łączą organizację ze wszystkim interesariuszami i ich oczekiwania. Przez kontekst wewnętrzny natomiast rozumie się strukturę organizacyjną, strategię, misję, cele organizacji, podział zadań, zasoby, kulturę organizacyjną czy kontrakty biznesowe. Dokładne zdefiniowanie kontekstu, w jakim działa organizacja pozwala na kolejnych etapach ustalić kryteria oceny ryzyka i jego akceptacji oraz ocenić wpływ zagrożeń na organizację i jej cele.

WAŻNE: Określenie zewnętrznych i wewnętrznych kwestii, które są istotne dla celu i które wpływają na zdolność do osiągnięcia zamierzonych wyników systemu zarządzania bezpieczeństwem informacji stanowi wymóg ISO 27001 wskazany w punkcie 4 Kontekst organizacji.

2. IDENTYFIKACJA RYZYKA

Identyfikacja ryzyka, czyli proces wyszukiwania, rozpoznawania i opisywania ryzyka (PN-EN ISO/IEC 27000:2014) polega na określeniu przyczyn i sposobów materializacji niepożądanych zdarzeń. Obejmuje on ustalenie zasobów (aktywów) informacyjnych, zagrożeń i źródeł ich powstawania.

Na tym etapie identyfikuje się również podatności oraz potencjalne skutki i straty związane z niepożądanymi zdarzeniami.

Kluczem do sukcesu na tym etapie jest właściwe i bardzo dokładne zinwentaryzowanie aktywów, czyli wszystkiego, co posiada dla organizacji wartość i jest nośnikiem informacji. Najczęściej wyróżnia się następujące kategorie aktywów:

1. informacyjne (dokumenty, bazy danych),
2. fizyczne (sprzęt komputerowy, budynki, urządzenia komunikacyjne),
3. oprogramowanie (systemy operacyjne, aplikacje),
4. personel (jego wiedza, doświadczenie i umiejętności),
5. dobra niematerialne (reputacja, wizerunek).

Kolejną rzeczą, na którą należy zwrócić uwagę, jest wskazanie dla każdego z aktywów właściciela, czyli osoby odpowiedzialnej za jego utrzymanie, korzystanie i bezpieczeństwo.

Po określeniu aktywów i przypisaniu im właścicielstwa następuje moment identyfikowania potencjalnych zagrożeń, czyli zdarzeń (losowych, umyślnych, nieumyślnych), które mogą oddziaływać na bezpieczeństwo aktywa. Dobrze jest także określić podatności aktywa, czyli inaczej mówiąc słabości lub luk w systemie przetwarzania informacji, które umożliwiają zmaterializowanie się danego zagrożenia.

3. ANALIZA RYZYKA

Analiza ryzyka to proces dążący do poznania charakteru ryzyka oraz określenia jego poziomu. Najczęściej sprowadza się on do określenia prawdopodobieństwa oraz skutków zaistnienia zidentyfikowanego ryzyka. Zaleca się, aby podczas oceny prawdopodobieństwa zaistnienia określonych zagrożeń rozważyć:

- źródło zagrożenia,
- możliwości dostępne dla potencjalnych atakujących,
- atrakcyjność i wrażliwość zasobów dla dla potencjalnych atakujących,
- lokalizacje,
- możliwość wystąpienia ekstremalnych warunków atmosferycznych,
- czynniki determinujące powstawania błędów i pomyłek.

Przy ocenie skutków należy mieć na uwadze zarówno te bezpośrednie jak koszty odtworzenia utraconych aktywów, konfiguracji, instalacji zasobu czy straty finansowe i wizerunkowe poniesione jako konsekwencja zawieszenia/braku dostępności usługi oraz pośrednie jak naruszenie obowiązków umownych, ustawowych czy kodeksów postępowania.

Na tym etapie dokonujemy również oszacowania wielkości ryzyka na podstawie kombinacji prawdopodobieństwa wystąpienia zagrożenia oraz jego skutków.

4. OCENA RYZYKA

Ocena ryzyka to zgodnie ze wskazaniem normy proces porównania wyników analizy ryzyka z kryteriami ryzyka (poziomy odniesienia, względem których określa się ważność ryzyka). Etap ten dostarcza informacji czy dane ryzyko jest dla organizacji akceptowalne. Pozwala on także na uszeregowanie ryzyk zgodnie z ich wartością oraz nadanie priorytetów postępowania z nimi.

5. POSTĘPOWANIE Z RYZYKIEM

Proces postępowania z ryzykiem, czyli jego modyfikacji za pomocą różnych strategii, w tym:

- redukcja ryzyka – obniżenie ryzyka do poziomu akceptowalnego dla organizacji poprzez dobór i zastosowanie odpowiednich czy to technicznych, czy organizacyjnych środków bezpieczeństwa dobranych adekwatnie do skali ryzyka oraz zasobów organizacji,
- unikanie – poprzez podjęcie działań zmierzających do zmodyfikowania lub całkowitego zaprzestania danej aktywności generującej ryzyko,
- przeniesienie – zlecenie czynności tworzącej ryzyko podmiotom zewnętrznym lub wykup polisy ubezpieczeniowej,
- utrzymanie – akceptacja ryzyka na stwierdzonym poziomie, poprzez podjęcie świadomej decyzji o niestosowaniu w danym momencie żadnych działań mających na celu redukcję ryzyka czy jego przeniesienie.

Bez względu, na którą z powyższych strategii zdecyduje się organizacja, powinna ona udokumentować swoje stanowisko w tzw. planie postępowania z ryzykiem, o którym mowa w punkcie 6.1.3 standardu ISO 27001. Plan powinien być zaakceptowany przez właściciela ryzyka i weryfikowany w trakcie i po jego zakończeniu w celu weryfikacji skuteczności i efektywności zaplanowanych prac.

6. AKCEPTACJA RYZYKA

Po wdrożeniu planu postępowania z ryzykiem następuje etap akceptacji tzw. ryzyka szczątkowego (rezydualnego) pozostałego po wdrożeniu zabezpieczeń. Ryzyko szczątkowe to takie, którego nie możemy już wyeliminować, a względem, którego najwyższe kierownictwo ustaliło i przyjęło kryteria akceptacji.

7. INFORMOWANIE O RYZYKU

Informowanie o ryzyku, czyli proces przekazywania wiedzy uczestnikom procesu (pracownikom zaangażowanym w dany proces, korzystającym z danego zasobu) o bieżącym statusie ryzyka. Mechanizmy, zgodnie z którymi ww. informacje są przekazywane, powinny być zaprojektowane już na etapie budowania systemu zarządzania ryzykiem. Powinny one zapewniać dostępność informacji właściwym osobom, w określonym czasie oraz pozwalać na wymianę wiedzy, oraz konsultacje. Istotą informowania ryzyku jest zapewnienie, że każdy właściciel ryzyka jest świadomy swojej roli oraz zakresu obowiązków i odpowiedzialności.

8. MONITOROWANIE I PRZEGLĄD RYZYKA

Jako że zarządzanie ryzykiem jest procesem ciągłym, to duże znaczenie w procesie zarządzania ryzykiem przypisuje się właśnie monitorowaniu oraz przeglądowi ryzyk. Etap ten ma za zadanie:

a) odpowiedzieć na pytanie: czy system zarządzania ryzykiem spełnia założone cele, czy polityki i procedury ustanowione w jego ramach są nadal aktualne, odpowiednie i wydajne;

b) zapewnienie, że wszystkie nowe ryzyka zostaną w odpowiednim czasie zidentyfikowane oraz ustanowione wobec nich priorytety działania.

Monitorowanie oraz przegląd ryzyk powinien być prowadzony w kontekście nowych aktywów, zagrożeń i podatności, a także incydentów związanych z naruszeniem bezpieczeństwa informacji. W sytuacji odnotowania jakichkolwiek zmian czynników wpływających na ryzyko należy dokonać ponownego przeglądu ryzyk oraz zaktualizowania ich wartości, jeżeli jest to uzasadnione.

Metody szacowania ryzyka

Powszechnie wyróżnia się trzy główne metody szacowania ryzyka:

- ilościowa,
- jakościowa,
- mieszana.

Metoda ilościowa polega na ocenie prawdopodobieństwa oraz skutków wystąpienia ryzyka poprzez nadanie im konkretnych wartości liczbowych. Zaletami metod ilościowych jest powtarzalność i względna obiektywność wyników, dzięki czemu mogą być one porównywane w czasie.

Do metod ilościowych zalicza się między innymi techniki: drzewo zdarzeń (Events Tree Analysis), drzewo błędów (Faults Tree Analysis) oraz FMEA.

Metoda jakościowa polega na indywidualnej ocenie ryzyka na podstawie doświadczenia, wiedzy oraz dobrych praktyk. Metoda ta wykorzystuje subiektywne miary i oceny takie jak wartości opisowe poziomów (niski, średni, wysoki). Korzyści metod jakościowych to:

- brak konieczności ilościowego określenia skutków i częstotliwości wystąpienia zagrożeń,
- wskazanie ogólnych obszarów ryzyka, na które konieczne jest zwrócenie uwagi,
- możliwość uwzględnienia takich jak np. wizerunek organizacji, jej kultura.

Zalety stosowania podejścia opartego na ryzyku

Podejście oparte na ryzyku coraz częściej wykorzystywane jest w różnych sferach życia organizacji, ponieważ niesie ze sobą wymierne korzyści. Główną zaletą zarządzania przez ryzyko jest to, że to organizacja dobiera środki bezpieczeństwa (czy to techniczne, czy organizacyjne) adekwatnie do stwierdzonego w danym czasie ryzyka z uwzględnieniem jej apetytu na ryzyko oraz

zasobów, którymi w danym momencie dysponuje. Zabezpieczenia są też adekwatne do skali działalności. Daje to również możliwość optymalizacji kosztów poprzez wczesne reagowanie na anomalie, a wręcz przyjęcie z postawy reaktywnej na zapobiegawczą. Wśród innych korzyści na płynących ze wdrożenia systemu zarządzania ryzykiem są:

- podejmowanie świadomych decyzji przez kierownictwo,
- zmniejszenie liczby i skali ryzyk,
- wzrost zaufania klientów i innych stron zainteresowanych,
- ujednolicenie podejścia od oceny ryzyka i reakcji na nie poprzez wdrożenie jednolitej metody oceny w różnych obszarach organizacji.

Podsumowanie

Zarządzanie ryzykiem w bezpieczeństwie informacji opiera się na odpowiednim zaplanowaniu, organizacji kierowania oraz kontrolowaniu zasobów. Wymaga zaangażowania oraz współpracy wszystkich stron przetwarzających informacje w celu określenia kryteriów akceptacji, wymagań oraz wyboru opcji postępowania z ryzykiem. Oprócz tego istotną rolę w obszarze zarządzania ryzykiem przypisuje się kierownictwu organizacji, które odpowiedzialne jest za kształtowanie oraz wzmacnianie wśród pracowników poczucia świadomości występowania zagrożeń, oraz potrzeby przeciwdziałania sytuacjom kryzysowym.

Warto również zauważyć, że podejście oparte na ryzyku i zarządzanie przez ryzyko nie jest cechą charakterystyczną jedynie dla norm z serii ISO. Również koncepcja Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zbudowana jest na tym podejściu, dając administratorom swobodę w wyborze zabezpieczeń i ich racjonalizację w zależności od skali ryzyka, charaktery danych czy organizacji.

Z doświadczenia LexDigital wynika, że system zarządzania ryzykiem będzie przynosił wymierne efekty tylko wówczas, jeżeli zostanie w odpowiedni sposób zaplanowany i ustanowiony. Ważna jest również komunikacja jego istoty i korzyści wśród personelu. Warto także na koniec podkreślić, że nie ma jednej uniwersalnej metody szacowania ryzyka, a dochodzenie do tej odpowiedniej dla organizacji również jest procesem, który może trwać nawet kilka lat i ewoluować wraz z organizacją.

Plan kontroli sektorowych UODO

Urząd Ochrony Danych Osobowych (UODO) przyjął plan kontroli sektorowych na 2024 rok. Kontrolom będą podlegać:

- organy przetwarzające dane osobowe w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym (SIS/VIS);
- podmioty, które przetwarzają dane osobowe przy użyciu aplikacji internetowych (webowych);
- podmioty prywatne, w kontekście prawidłowości spełniania obowiązku informacyjnego określonego w art. 13 i 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679.

Kontrole te są konieczne ze względu na rosnące zagrożenia naruszania przepisów o ochronie danych osobowych w tych sektorach oraz duże społeczne zainteresowanie tymi problemami.

Źródło: https://bit.ly/49hrJ6O

Informacja o monitoringu pracowników musi być oddzielnym dokumentem. Tak twierdzi UODO.

Urząd Ochrony Danych Osobowych (UODO) wydał stanowisko dotyczące informowania pracowników o monitoringu w miejscu pracy. Zgodnie z nim, nie wystarczy, że pracownik zapoznał się z regulaminem pracy, który zawiera zasady monitoringu. Pracodawca musi także indywidualnie poinformować pracownika o celu, zakresie i sposobie monitoringu. Ponadto, informacje o monitoringu muszą być zindywidualizowane, tj. dostosowane do konkretnego pracownika i rodzaju monitoringu, którego dotyczy. Wszystkie formy monitoringu, nawet te dotyczące wyjątkowo niektórych pracowników, powinny być jasno przekazane. Jest to konieczne z uwagi na zasadę przejrzystości wynikającą z RODO. Dlatego też, pracodawca powinien dostarczyć nowemu pracownikowi trzy dokumenty: zapoznanie z regulaminem pracy, informację o monitoringu oraz klauzulę informacyjną zgodnie z art. 13 RODO.

Źródło: https://bit.ly/3uB9MRs

Pierwsze w swoim rodzaju prawo dotyczące sztucznej inteligencji od krajów UE

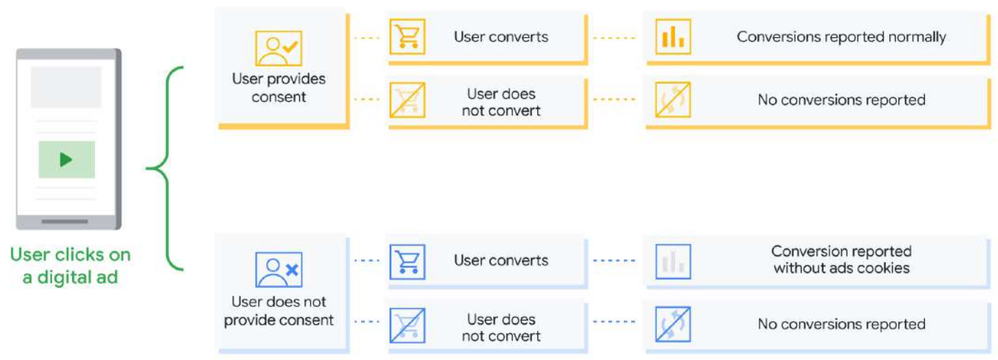
Ambasadorowie UE zatwierdzili pierwsze na świecie przepisy dot. sztucznej inteligencji. Porozumienie polityczne osiągnięto w grudniu. Belgia przedstawiła ostateczny tekst 24 stycznia. Francja, Niemcy i Włochy chciały lżejszych regulacji dla potężnych modeli AI. Parlament Europejski opowiadał się za ostrzejszymi zasadami. Francja ostatecznie poparła tekst "z surowymi warunkami". UE ma wpływ na to, jak ustawa będzie wdrażana. Działanie AI Act rozpocznie się 20 dni po opublikowaniu w Dzienniku Urzędowym, z zakazami praktyk będącymi wyjątkami, a obowiązki dla modeli AI - po roku. Pełne wdrożenie przepisów nastąpi po dwóch latach, z wyjątkiem klasyfikacji systemów AI podlegających ocenie zgodności przez strony trzecie, które zostały opóźnione o kolejny rok.

Źródło: https://bit.ly/3I77jRO

Nowy tryb zbierania zgód od Google Analytics. Od marca możesz nie wyrażać zgody na reklamy

Google Analytics wprowadza "Consent Mode" - nowy tryb zbierania zgód dla spersonalizowanych reklam, obowiązkowy od marca 2024. Zgoda użytkowników nadal będzie potrzebna, pomimo możliwości śledzenia bez plików cookie. Tryb deleguje uzyskiwanie zgód od Google do operatorów stron internetowych. Jest on konieczny dla użytkowników chcących korzystać z usług Google, np. Google Ads. Wdrożenie powinno odbywać się zgodnie z polityką Google EU user consent policy. Bez udzielenia zgody Google Analytics nie jest uruchamiane, a po uzyskaniu zgody są zapisywane i odczytywane pliki cookie. Odrzucenie zgody oznacza, że Google Analytics może być nadal uruchamiane, ale bez zapisywania plików cookie.

Źródło: https://bit.ly/3uBa8aK



EDPB ułatwia audyt stron www z nowym narzędziem

Europejski Komitet Ochrony Danych Osobowych (EDPB) wprowadził narzędzie do audytu stron internetowych, pomagające sprawdzić, czy są zgodne z prawem. Narzędzie to jest dostępne dla organów ochrony danych, kontrolerów i przetwarzających. Jest to oprogramowanie o otwartym kodzie źródłowym, umożliwiające przygotowywanie, przeprowadzanie i ocenę audytów oraz generowanie raportów. Ułatwia ono egzekwowanie przepisów i sprawdzanie zgodności. Oprogramowanie zostało rozwinięte w ramach EDPB Support Pool of Experts i będzie regularnie aktualizowane.

Źródło: https://bit.ly/3SJ9Vu3

Dyrektor finansowy firmy nabrał się na DeepFake oszustwo. Korporacja straciła 25,6 mln dolarów.

"Wszyscy wyglądali na prawdziwych". Międzynarodowa korporacja z Hongkongu straciła 25,6 miliona dolarów przez fałszywą rozmowę wideo. Oszuści zorganizowali rozmowę, na którą zaprosili dyrektora finansowego firmy. Oprócz niego na tym spotkaniu wszyscy pozostali uczestnicy nie byli prawdziwi, ale stworzeni za pomocą technologii DeepFake, w tym dyrektor finansowy firmy.

Na fałszywym spotkaniu "szefowie" nakazali dyrektorowi przelać pieniądze na kilka fałszywych kont, co podwładny zrobił. Co charakterystyczne, najpierw próbowali go zmusić do przelania pieniędzy za pomocą e-maili phishingowych, ale wtedy pracownik podejrzewał, że coś jest nie tak. Kiedy maile nie zadziałały, specjalnie dla niego oszuści zorganizowali fałszywego calla z cyfrowymi kopiami szefostwa i kolegów. Później policja dowiedziała się, że w podobny sposób oszuści próbowali zaatakować kilku pracowników korporacji, dopóki nie znaleźli najbardziej łatwowiernego.

Źródło: https://bit.ly/3wr74yp

Dane 33 milionów francuzów skradzione w wyniku ataku

W wyniku ataku hakerskiego na francuskie firmy ubezpieczeniowe Viamedis i Almerys, doszło do masowego naruszenia bezpieczeństwa danych. Około 33 miliony klientów zostało dotkniętych. Skradzione dane zawierają m.in. daty urodzenia, stan cywilny, numery ubezpieczenia. Pomimo poważności incydentu, dane bankowe, medyczne oraz numery kontaktowe nie zostały skompromitowane. Atakujący wykorzystali skradzione dane od pracowników służby zdrowia, by dostać się do systemów firm. CNIL współpracuje z firmami, by powiadomić wszystkich poszkodowanych, co jednak zajmie trochę czasu ze względu na liczbę klientów. Możliwe, że system "tiers payant", w którym pacjenci nie muszą opłacać pełnej kwoty usług medycznych z góry, będzie niedostępny przez pewien czas dla dostawców, ale pacjenci wciąż będą mieli do nich dostęp. Francuski organ danych

wysłał ostrzeżenie przed phishingiem, w związku z dużą ilością skradzionych danych. Trwa pełne dochodzenie w celu ustalenia, jak doszło do tej masowej usterki i czy Viamedis lub Almerys ponoszą winę.

Źródło: https://bit.ly/3wfXrmh

Munich Security Report: postrzegane zagrożenie cyberatakami osiąga rekordowy poziom

Kraje G7 uważają ataki w sieci za drugie co do wielkości zagrożenie, zaraz po ekstremalnych warunkach pogodowych. Tak wynika z raportu przed Konferencją Bezpieczeństwa w Monachium. W raporcie tym każdego roku omawia się aktualne problemy związane z bezpieczeństwem i są one podstawą do dyskusji. W tym roku raport pokazuje, że ryzyko ataków w sieci jest teraz największe.

"Technologia kiedyś pomagała w rozwoju gospodarczym i łączeniu ludzi na świecie. Dziś stała się polem walki między różnymi systemami" - powiedział Tobias Bunde, który zajmuje się badaniami i polityką na Konferencji Bezpieczeństwa w Monachium.

Według badania MSI, zagrożenie atakami w sieci wzrosło o pięć miejsc. Ryzyko ataków w sieci i zmiany klimatyczne zawsze były wysoko oceniane. To ryzyka systemowe, dlatego pozostaną priorytetem, w przeciwieństwie do innych zagrożeń, takich jak pandemia, z którą trzeba się stale zmagać — powiedział Weber.

Wyniki badań należy też rozważyć w kontekście relacji medialnych — powiedział Müller-Quade, wyjaśniając, że gdyby doszło do spektakularnego ataku hakerskiego przed badaniem, ryzyko na pewno zostałoby ocenione wyżej.

Wyniki dają wgląd w bieżące postrzeganie ryzyka, silnie zależne od tematów w mediach.

Źródło: https://bit.ly/4bBxxJP

Komisja Europejska wszczyna dochodzenie w sprawie Tik Tok

Europejska Komisja planuje wszcząć dochodzenie w sprawie TikToka w najbliższych tygodniach z obawą, że zmiany wprowadzone przez firmę w celu zgodności z rozporządzeniem dotyczącym usług cyfrowych (DSA) UE nie są wystarczające do ochrony nieletnich użytkowników - donosi Bloomberg. TikTok nie otrzymał jeszcze informacji od Komisji Europejskiej o wszczęciu dochodzenia i regularnie dialoguje z władzami UE - powiedział rzecznik TikToka. Dochodzenie może skutkować nałożeniem kary na właściciela TikToka, chińską firmę ByteDance, chociaż UE może jeszcze zdecydować się nie kontynuować dochodzenia.

DSA, które weszło w życie w 2022 roku, nakłada nowe zasady dotyczące moderowania treści, prywatności użytkowników i przejrzystości. Każdej firmie, naruszającej przepisy grozi kara w wysokości do 6% rocznego obrotu globalnego. UE rozpoczęła swoje pierwsze formalne dochodzenie na podstawie DSA w ubiegłym roku w sprawie firmy X, podejrzanej o naruszenia dotyczące treści po ataku Hamas na Izrael.

Źródło: https://reut.rs/4bCAVnP

Polska

Prezes Urzędu Ochrony Danych Osobowych ponownie analizował naruszenie RODO przez Morele.net z powodu wycieku danych i nałożył na administratora karę ponad 3,8 mln zł. Po uchyleniu decyzji przez Naczelnego Sądu Administracyjnego, UODO przeprowadził ponowne postępowanie, które potwierdziło niewystarczające zabezpieczenia techniczne i brak procedur reagowania na nietypowe zachowania. Analiza wykazała, że spółka nie szyfrowała części danych, nie miała dwuskładnikowego uwierzytelniania, ani monitoringu ruchu sieciowego. Braki te przyczyniły się do dwóch nieautoryzowanych dostępów z zewnątrz. UODO uznał konieczność nałożenia kary, uwzględniając wytyczne Rady Ochrony Danych Osobowych.

Źródło: https://bit.ly/3UIAa6F

Świat

Austriacki organ ochrony danych nałożył karę w wysokości 20 000 euro na administratora za bezprawne wykorzystanie kamer rejestrujących pracowników w miejscu pracy oraz brak prowadzenia rejestru działań przetwarzania zgodnie z art. 30 RODO. Skarżący, byli pracownicy restauracji, zauważyli, że są rejestrowani przez kamerę w miejscu pracy, a nagrania były dostępne dla pracodawcy. Administrator twierdził, że kamery służyły do ochrony mienia i pracowników, a przetwarzanie było oparte na zgodzie pracowników. Organ uznał, że kamery rejestrowały obszar kuchni, co było bezprawne, i że administrator nie prowadził rejestru działań przetwarzania. Na decyzję organu zostało złożone odwołanie, a postępowanie sankcjonujące jest w toku.

Źródło: https://bit.ly/3we4gEO

Cypryjski organ ochrony danych nałożył karę w wysokości 45 000 euro na Uniwersytet Otwarty Cypru za brak odpowiednich środków bezpieczeństwa zgodnie z art. 32 RODO. Kara została nałożona po tym, jak Uniwersytet zgłosił naruszenie danych osobowych do organu ochrony danych (Komisarz ochrony danych osobowych, DPC) zgodnie z art. 33 RODO. Dodatkowo, 11 skarg zostało złożonych przez osoby, których dane wyciekły w wyniku incydentu.

Komisarz rozpoczął śledztwo w sprawie i ustalił, że wyciekłe dane dotyczyły studentów, absolwentów i innych partnerów uczelni, a były one przechowywane na serwerach uczelni i ogólnie przetwarzane przez jej pracowników.

W swoich wnioskach przesłanych do DPC, uniwersytet przedstawił listę działań, które zamierza wdrożyć do 2026 roku w celu poprawy bezpieczeństwa swoich operacji przetwarzania danych. Po dalszych dochodzeniach DPC doszedł do wniosku, że uniwersytet nie zastosował odpowiednich środków technicznych i organizacyjnych, naruszając tym samym art. 32 RODO oraz zasadę odpowiedzialności określoną w art. 5(2) RODO.

Biorąc pod uwagę art. 83 RODO oraz wszystkie powyższe okoliczności, a także fakt, że kontroler należy do szeroko pojętego sektora publicznego, DPC uznał za stosowne nałożenie kary w wysokości 45 000 euro na uniwersytet.

Źródło: https://bit.ly/3UF86kv

Holenderski organ ochrony danych nałożył 10 milionów euro kary na Ubera za brak przejrzystości w polityce prywatności i utrudnienia w korzystaniu z praw RODO przez kierowców. Organizacja LDH złożyła skargę w imieniu 172 kierowców, a CNIL przekazał ją holenderskiemu organowi nadzorczemu. AP stwierdził, że formularz Ubera do korzystania z praw RODO nie był łatwo dostępny, co naruszało art. 12 ust. 2 RODO. AP uznał także, że Uber nie dostarczał informacji w jasny i prosty sposób, co naruszało art. 12 ust. 1 RODO. Polityka prywatności Ubera była zbyt ogólna w kwestii okresów retencji danych, nie wspominając

o przekazach danych do państw trzecich ani o przenośności danych, co naruszało art. 13 i 15 RODO. W rezultacie AP nałożył 10 milionów euro kary na Ubera za dwa rodzaje naruszeń, uwzględniając fakt, że Uber naprawił niektóre naruszenia po raporcie AP.

Źródło: https://bit.ly/49CKr8F

Hiszpańska Agencja Ochrony Danych nałożyła na EasyJet karę 8 000 euro za opóźnienie w odpowiedzi na żądanie dostępu do danych osobowych. Wniosek został złożony 28/12/2021, a EasyJet odpowiedziało dopiero 01/04/2022. Firma tłumaczyła to urlopem pracowników i błędnym wysłaniem wniosku. DPA zwróciła uwagę, że odpowiedź powinna nadejść w ciągu miesiąca. Pomimo pierwszej odpowiedzi EasyJet w grudniu 2021, firma nie dostarczyła pełnych informacji aż do kwietnia 2022. DPA orzekła karę 8 000 euro, którą EasyJet dobrowolnie zapłaciło.

Źródło: https://bit.ly/42ELT8n

Hiszpański organ ochrony danych nałożył karę w wysokości 5000 euro na administratora za udostępnienie danych osobowych pracownika na Whatsapp. Skarżący wysłał administratorowi profesjonalny e-mail dotyczący kwestii związanej z pracą. Administrator umieścił zrzut ekranu tego e-maila na profilu firmowym skarżącego na Whatsappie, zawierając jego imię i nazwisko oraz pytanie dotyczące sprawy pracowniczej. Mimo kilkukrotnego próbowania skontaktowania się z administratorem, ten nie udzielił odpowiedzi. Organ nałożył karę za naruszenie art. 5 ust. 1 lit. f RODO, uznając, że administrator nie zapewnił bezpieczeństwa danych pracownika, udostępniając je na firmowym koncie Whatsapp. Organ dał administratorowi możliwość udziału w wysłuchaniu w ciągu 10 dni od decyzji. Jeśli administrator przyzna swoją odpowiedzialność, kara zostanie zmniejszona o 20% do 4000 euro. Jeśli nie odpowie na decyzję, organ uzna to za ostateczną decyzję i utrzyma karę w pierwotnej wysokości.

Źródło: https://bit.ly/42XNGFP

Dziękujemy za przeczytanie naszego Newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI