Bezpieczeństwo informacji — czy da się je osiągnąć?

W TYM WYDANIU:

LexDigital

www.lexdigital.pl

Natalia Dzieciuchowicz

Sprawozdanie Prezesa Urzędu Ochrony Danych Osobowych – trochę statystyk i ciekawostek

Jak co roku Prezes Urzędu ochrony Danych osobowych przedstawił sprawozdanie ze swojej działalności. Tegoroczne sprawozdanie obejmuje okres od 01.01. 2022 do 31.12.2022.

Zgodnie z ustawą z 10 maja 2018 r. o ochronie danych osobowych, Prezes przedłożył sprawozdanie Sejmowi Rzeczypospolitej Polskiej, Radzie Ministrów, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz Prokuratorowi Generalnemu.

Na mocy przepisu art. 59 ogólnego rozporządzenia o ochronie danych, sprawozdanie jest także udostępnione opinii publicznej, Komisji oraz Europejskiej Radzie Ochrony Danych. Obszerny dokument przedstawia najważniejsze ustalenia dotyczące zrealizowanych przez Prezesa UODO ustawowych zadań, do których należą: rozpatrywanie skarg, prowadzenie kontroli, opiniowanie projektów aktów prawnych, przyjmowanie zgłoszeń naruszeń ochrony danych i podejmowanie czynności wobec administratorów i podmiotów przetwarzających w celu powiadomienia osób, których dane zostały naruszone.

Prezes poinformował również o prowadzonej przez Urząd działalności edukacyjno-informacyjnej oraz uczestnictwie w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

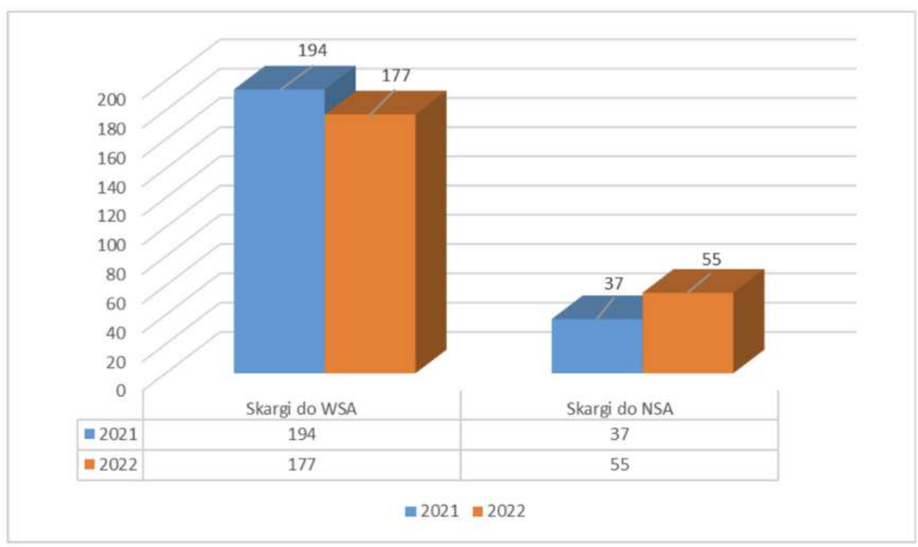
Skargi, naruszenia i kontrole prowadzone przez Urząd

Jednym z tematów ujętych w sprawozdaniu, a zawsze budzącym emocje jest temat skarg, naruszeń i kar nałożonych na administratorów danych w wyniku postępowań Urzędu. Do zadań jednostek organizacyjnych Urzędu Ochrony Danych Osobowych należy bowiem w szczególności: rozpatrywanie skarg w sprawach wykonania przepisów RODO i prowadzenie w tym zakresie postępowań administracyjnych, podejmowanie czynności w sprawie zgłaszanych przez administratorów naruszeń ochrony danych osobowych.

- **Orzecznictwo sądów administracyjnych w sprawach decyzji lub postanowień organu nadzorczego**

Na uwagę zasługuje fakt, że w roku 2022 odnotowano wzrost wydanych decyzji w sprawach skargowych w stosunku do lat poprzednich oraz zaobserwowano mniejszą liczbę wnoszonych skarg na decyzje organu do Wojewódzkiego Sądu Administracyjnego (WSA) w Warszawie.

W roku 2022 skarga taka została wniesiona w 177 przypadkach, zaś w roku 2021 odnotowano 194 takie skargi. Wzrósł natomiast wskaźnik zaskarżalności do Naczelnego Sądu Administracyjnego (NSA) wyroków wydanych w 2022 r. przez WSA w Warszawie w sprawach decyzji Prezesa Urzędu Ochrony Danych Osobowych dot. skarg. W roku 2022 do NSA wniesiono 55 skarg.



Wykres 1: Decyzje wydane w postępowaniach skargowych – zaskarżone do WSA w Warszawie i NSA.

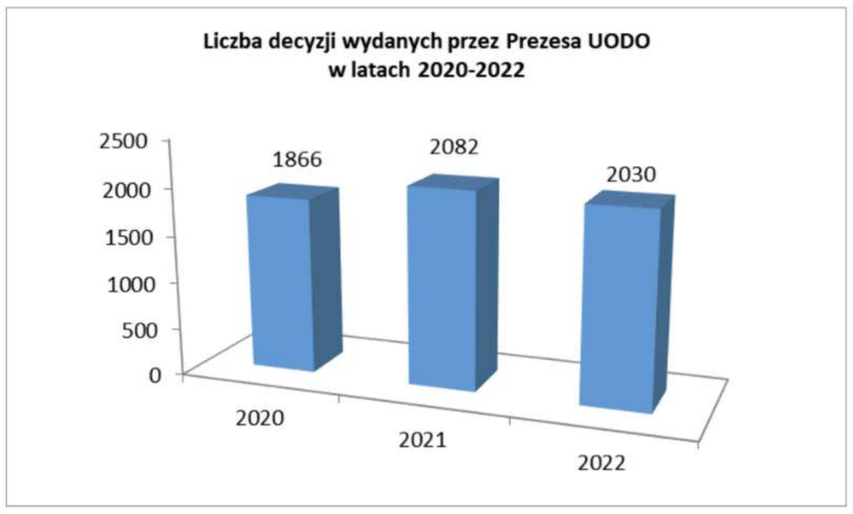
Źródło: Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2022

- **Decyzje administracyjne**

Postępowanie, dotyczące naruszenia przepisów o ochronie danych osobowych, wszczęte przez Prezesa UODO z urzędu lub na wniosek osoby zainteresowanej, toczy się według przepisów ustawy z 10 maja 2018 r. o ochronie danych osobowych, a w zakresie w tej ustawie nieuregulowanym, zgodnie z przepisami k.p.a.

W przypadku stwierdzenia naruszenia przepisów prawa, postępowanie to może zakończyć się wydaniem decyzji administracyjnej, mocą której Prezes Urzędu Ochrony Danych Osobowych m.in.: umarza postępowanie, odmawia uwzględnienia wniosku skarżącego, nakazuje przywrócenie stanu zgodnego z prawem, nakłada karę, upomnienie albo ostrzeżenie na administratora czy podmiot przetwarzający.

W roku 2022 Prezes UODO wydał 2030 decyzji administracyjnych, co jest liczbą porównywalną do roku 2021, w którym wydanych zostało 2082 decyzje administracyjne i o 164 więcej w stosunku do roku 2020, w którym wydanych było 1866 decyzji.



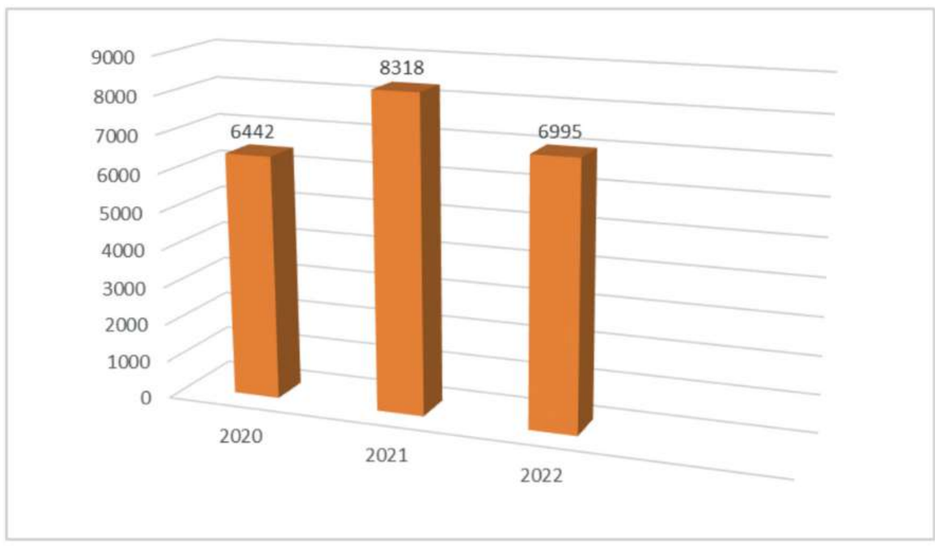
Wykres 2: Liczba decyzji wydanych przez Prezesa UODO w latach 2020-2022.

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

- **Skargi**

Zgodnie z art. 77 RODO, każda osoba, która uważa, iż przetwarzanie jej danych osobowych narusza przepisy RODO, może wnieść skargę do organu nadzorczego. W 2022 roku do Prezesa UODO wpłynęło 6995 takich skarg. Dla porównania, w 2021 roku było ich aż 8318. Każda skarga jest analizowana pod kątem spełniania wymogów formalnych (jeżeli bowiem skarga nie spełnia wymogów formalnych i po wezwaniu do uzupełnianie braków – nie zostały one uzupełnione – skarga nie jest rozpatrywana) i analizowana przez pracowników Urzędu w celu rozstrzygnięcia sprawy.

Urząd zbiera materiał dowodowy i na bieżąco informuje strony o postępach w toczącym się postępowaniu.



Wykres 3: Liczba skarg, które wpłynęły do UODO w latach 2020-2022.

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

Poniżej opisano przykłady skarg oraz decyzje Urzędu w sprawach istotnych z punktu widzenia pracodawcy:

- **Przetwarzanie przez pracodawcę danych osobowych pracownika w zakresie prywatnego numeru telefonu dla celów służbowych**

Urząd badał nieprawidłowości, polegające na przetwarzaniu przez pracodawcę prywatnego numeru telefonu komórkowego pracownika bez podstawy prawnej. Pracownik nie wyraził zgody na przetwarzanie jego danych osobowych w zakresie numeru telefonu dla celów służbowych, polegających na zapewnieniu bezpieczeństwa mienia administratora w ramach procesu aktywacji lub dezaktywacji systemu zabezpieczeń.

W związku z powyższym zwrócił się do Prezesa UODO z żądaniem nakazania administratorowi usunięcia danych osobowych skarżącego w zakresie jego numeru telefonu komórkowego.

Prezes UODO, po przeprowadzeniu postępowania administracyjnego wydał decyzję, na mocy której m.in. udzielił administratorowi upomnienia za naruszenie artykułu 5 ust. 2 RODO oraz artykułu 6 ust. 1 RODO, poprzez przetwarzanie danych osobowych w zakresie numeru telefonu komórkowego bez podstawy prawnej.

- **Przetwarzanie danych osobowych pracownika po zakończeniu zatrudnienia**

W tym przypadku Urząd oceniał skargę byłego pracownika na nieprawidłowości w procesie przetwarzania jego danych osobowych przez pracodawcę.

Polegały one na bezprawnym przetwarzaniu jego służbowego adresu e-mail pomimo wypowiedzenia mu umowy o pracę oraz odebrania mu dostępu do jego danych osobowych, w tym danych prywatnych, zgromadzonych w systemach spółki, w tym na skrzynce e-mailowej. Adres e-mail skarżącego był adresem przetwarzanym w związku z jego zatrudnieniem i wykorzystywany w celu realizacji przez niego obowiązków służbowych oraz w procedurze naliczania mu wynagrodzenia przez dział HR spółki do dnia upływu okresu wypowiedzenia.

Jak prawidłowo przetwarzać dane pracownika po zakończeniu zatrudnienia? Kliknij i sprawdź!

Po zaprzestaniu pełnienia jakiejkolwiek funkcji przez skarżącego spółka ustawiła automatyczną odpowiedź kierowaną do wszystkich osób podejmujących kontakt za pośrednictwem adresu e-mail skarżącego, informującą, że nie pełni już żadnych funkcji w spółce, a w celu uzyskania informacji należy kontaktować się za pośrednictwem nowego adresu.

Zablokowania adresu e-mail skarżącego, ustawienia wiadomości automatycznych, przekierowań oraz innych jego dostępów do systemów, dokonali upoważnieni pracownicy, którzy nie zapoznawali się z treścią korespondencji wpływającej na skrzynkę e-mailową. UODO osobowych pozytywnie ocenił działania administratora. Spółka legitymowała się prawnie uzasadnionym interesem uprawniającym ją do przetwarzania adresu e-mail skarżącego w okresie wypowiedzenia i po ustaniu zatrudnienia zgodnie z art. 6 ust. 1 lit. f) RODO. W toku przeprowadzonego postępowania dowodowego organ nie stwierdził, aby przetwarzanie naruszyło zasady przetwarzania danych określone w art. 5 ust. 1 RODO.

- **Pozyskiwanie przez pracodawców informacji o przyczynie zwolnienia lekarskiego.**

Prezes UODO otrzymywał również skargi, dotyczące pozyskiwania przez pracodawców informacji o specjalizacji lekarza wystawiającego skarżącym zwolnienia lekarskie, a następnie udostępnianie tej informacji osobom nieupoważnionym. Jak wskazano w jednej ze spraw, informacja o specjalizacji lekarza wystawiającego zwolnienie (psychiatria) była łatwa do pozyskania, poprzez wyszukanie jej w Internecie w oparciu o nazwisko lekarza.

Skarżący zarzucali przy tym, że pracodawcy przedstawiają ich sytuację zdrowotną w sposób prześmiewczy, ujawniają tego rodzaju dane w sposób celowy, przekazując je innym współpracownikom. W jednej ze spraw skarżąca wskazała, że w konsekwencji udostępnienia jej danych odczuwała brak komfortu pracy w środowisku, które poznało jej problemy chorobowe. Oceniając postępowanie pracodawców, Prezes UODO uznał, że takie działanie stanowiło naruszenie danych osobowych zaliczanych do szczególnych kategorii. Każde działanie pracodawcy, związane z przetwarzaniem danych, musi mieć swoje prawne uzasadnienie i odpowiadać istniejącym regulacjom prawnym.

Informacje dotyczące pracowników, w tym te odnoszące się do określonych zdarzeń, takich jak wystawienie zwolnienia lekarskiego, powinny być dostępne jedynie dla ograniczonego kręgu osób u danego pracodawcy.

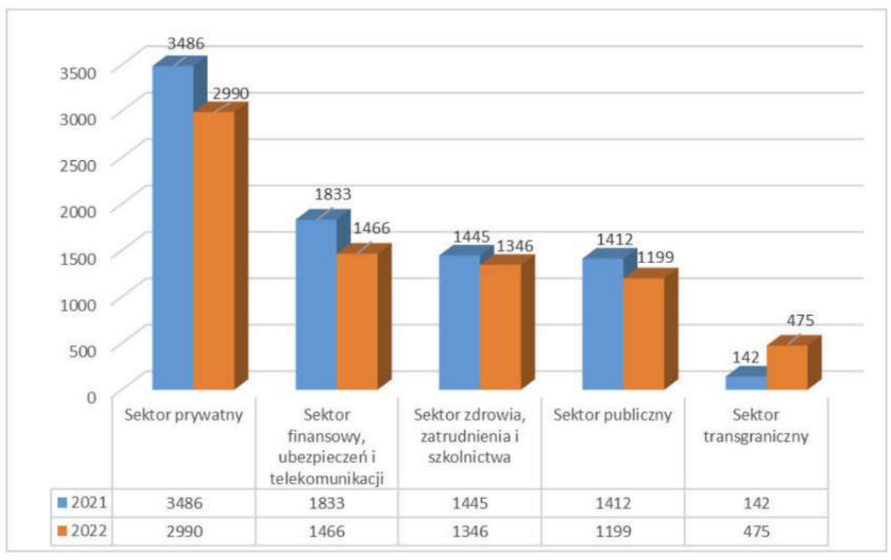
Do osób takich należą najczęściej osoby zarządzające zakładem pracy, osoby prowadzące sprawy osobowe, zatrudnienia i płac, radcy prawni świadczący dla pracodawcy pomoc prawną. Osoby te, w ramach wykonywanych obowiązków, są najczęściej upoważnione do przetwarzania danych innych pracowników, ponieważ wiąże się to ściśle z zakresem zadań, jakie wykonują w danym zakładzie pracy.

Prezes UODO w tego rodzaju sprawach zastosował wobec pracodawców upomnienia za naruszenie art. 9 ust. 1 oraz art. 5 ust. 1 lit. a) RODO.

- Bezprawne udostępnienie danych osobowych pracownika osobom trzecim.

Z analizy skarg z tego obszaru wynikało, że pracownicy często skarżą się na nieuprawnione udostępnienie ich danych osobowych przez pracodawców osobom trzecim. Zdaniem pracodawców udostępnianie danych osobowych nieuprawnionym podmiotom wynika często z braku odpowiedniego przeszkolenia personelu, chęci szybkiego zarządzania nieobecnościami w pracy, czy wreszcie z braku należytej uwagi dla przestrzegania przepisów RODO przez administratorów.

W jednej z prowadzonych spraw ustalono, że pracodawca bez podstawy prawnej poinformował kontrahenta spółki oraz osobę zatrudnioną u pracodawcy o fakcie przebywania skarżącej na zwolnieniu lekarskim. Ponadto pracodawca wykorzystywał do korespondencji służbowej prywatny numer jej telefonu. Pracodawca argumentował, że udostępnienie informacji o przebywaniu przez skarżącą na zwolnieniu lekarskim było podyktowane koniecznością usprawiedliwienia kontrahentowi faktu, że w zastępstwie skarżącej jej obowiązki będzie wykonywać inna osoba oraz usprawiedliwienia faktu długotrwałego braku kontaktu z kontrahentem pracodawcy. Ponadto pracodawca przyznał, że korespondencja być może mogła omyłkowo i niecelowo być prowadzona z kontem użytkownika jednej z aplikacji, przypisanym do jej numeru prywatnego.



Wykres 5: Liczba skarg, które wpłynęły do UODO w latach 2021-2022 z podziałem na sektory.

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

Prezes UODO stwierdził naruszenie art. 6 ust. 1 RODO, polegające na przetwarzaniu bez podstawy prawnej danych osobowych skarżącej w zakresie prywatnego numeru telefonu oraz naruszenie art. 9 ust. 1 RODO, polegające na udostępnieniu na rzecz osób nieuprawnionych danych osobowych dotyczących zdrowia (informacji o fakcie przebywania na zwolnieniu lekarskim) kontrahentowi pracodawcy oraz nieupoważnionej do przetwarzania danych osobowych skarżącej osobie, zatrudnionej u pracodawcy.

Oprócz wyżej przytoczonych przykładów skarg, które były rozpatrywane przez Urząd, wpływały do niego również skargi na działania banków, podmiotów udzielających kredytów, firm windykacyjnych czy ubezpieczycieli.

Do Urzędu Ochrony Danych Osobowych wpłynęło również 28 skarg na działanie Urzędu. Przeważnie skargi składane były w toku prowadzonych postępowań i dotyczyły przewlekłego załatwiania spraw lub domniemanej bezczynności Prezesa UODO.

Urząd, w swoim sprawozdaniu, nie zajął stanowiska w tej sprawie.

Kontrole przestrzegania przepisów o ochronie danych osobowych

Prezes UODO, na mocy art. 78 Ustawy o ochronie danych osobowych może przeprowadzać kontrole przestrzegania przepisów o ochronie danych osobowych. Mogą to być kontrole planowe lub przeprowadzane w ramach monitorowania przestrzegania przepisów RODO (np. na podstawie skarg, które wpływają do Urzędu). W 2022 Prezes UODO przeprowadził kontrole w 40 podmiotach.

Kontrole planowe, przeprowadzone zgodnie z planem kontroli sektorowych, który każdego roku sporządzany jest przez Urząd, objęły podmioty z sektora bankowego, jak również podmioty, które przetwarzają dane osobowe przy użyciu aplikacji mobilnych. Urząd uznał, że te właśnie grupy warto poddać kontroli ze względu na liczne skargi, które wpłynęły do Urzędu oraz znaczną liczbę naruszeń zgłoszonych w obszarze funkcjonowania tych grup podmiotów.

Ponadto kontrolami zostały objęte organy administracji rządowej i samorządowej, uczelnie wyższe, stowarzyszenie, placówki medyczne i jeden z konsulatów RP. Przeprowadzone kontrole wynikały również ze zgłoszonych naruszeń ochrony danych. Rok 2022 zakończył się przeprowadzeniem 8 postępowań kontrolnych, zapoczątkowanych w wyniku wspomnianego naruszenia.

Dodatkowo Prezes UODO skierował 24 pisma w zakresie sprawdzenia prawidłowości powołania i funkcjonowania Inspektorów Ochrony Danych. Przedmiot zainteresowania stanowiły informacje o sposobie zapewnienia kontaktu z IOD, jego umiejscowieniu w strukturze administracyjnej, kompetencjach, zaangażowaniu w sprawy dotyczące ochrony danych osobowych oraz co najważniejsze, o zapewnieniu gwarancji niezależności i możliwości prawidłowego realizowania obowiązków.

Podsumowanie

Powyżej przedstawiono tylko skrawek informacji, które zostały przekazane w sprawozdaniu Prezesa Urzędu Ochrony Danych osobowych. Ilość wpływających do Urzędu zgłoszeń, skarg, zapytań pokazuje coraz większą świadomość społeczeństwa w zakresie konieczności ochrony prywatności i jest to sygnał dla administratorów danych, że ochrona danych osobowych powinna być dzisiaj podstawowym elementem codziennego życia każdej organizacji.

Olga Ograbisz

Szczegóły i kwestie, na które należy zwrócić uwagę podczas wdrożenia ISO 27001

Informacja, jako najważniejsza wartość biznesu

Informacja, była jest i będzie jedną z najcenniejszych wartości, która stanowi niejako motor napędowy dla funkcjonowania rynku. W dobie praktycznie nieskrępowanej wymiany informacji pomiędzy najbardziej oddalonymi od siebie punktami świata, staramy się ją chronić za wszelką cenę, a umiejętność pozyskania informacji staje się kluczowym elementem implikującym sukces rynkowy przedsiębiorstwa. Informacja jest bowiem postrzegana jako najcenniejszy zasób niosący za sobą wiedzę dla podejmowanych działań i decyzji. Mało tego — złe zarządzanie informacją może doprowadzić do problemów finansowych, upadku przedsiębiorstwa czy nawet kłopotów z prawem. Może stać się ona również obiektem przestępczości.

Słowo informacja pochodzi od łacińskiego słowa informatio oznaczającego wyobrażenie, wizerunek, zarys pojęcie. Obecnie pojęcie interdyscyplinarne i szeroko rozumiane. Słownik języka polskiego definiuje informację jak coś, co powiedziano lub napisano o kimś, lub o czymś, lub inaczej dane przetwarzane przez komputer. Uniwersalną definicję wprowadzono w ramach Open Archival Information

System (OAIS), która mówi o tym, że informacja to wiedza dowolnego rodzaju, którą można się dzielić niezależnie od formy użytej dla jej wyrażenia. Według norm z serii ISO informacja definiowana jest jako aktywo przybierające różne formy (drukowaną, pisaną, elektroniczną, audio i video, ustną), które ma wartość dla organizacji i dlatego właśnie należy ją chronić.

Coraz bardziej urzeczywistniające się zapotrzebowanie na ochronę informacji, często wynikające bezpośrednio z przepisów prawa, stało się podwaliną do opracowania standardów bezpieczeństwa informacji. Do najpopularniejszych standardów o poruszanej tematyce należy PN-EN ISO/IEC 27001:2017 Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania., która w najbliższym czasie będzie pomału zastępowana standardem PN-EN ISO/IEC 27001:2022 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności. System zarządzania bezpieczeństwem informacji. Wymagania.

Obie normy zostały opracowane dla dostarczenia wymagań w zakresie ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji, jest dedykowana każdej organizacji bez względu na przedmiot czy skalę działalności, rozmiar, formę dzielności czy sposób zarządzania.

Bezpieczeństwo informacji

Bezpieczeństwo informacji to nic innego jak zapewnienie trzech głównych atrybutów: poufności, integralności i dostępności danych, przy równoczesnym uwzględnieniu takich cech jak rozliczalność, autentyczność, niezaprzeczalność i niezawodność. Najważniejsze w zachowaniu bezpieczeństwa jest zatem właściwe zarządzanie i zastosowanie poszczególnych środków, które mamy w arsenale. To wiąże się z rozpatrzeniem szerokiej gamy zagrożeń, które mogą z różnym prawdopodobieństwem wystąpić w organizacji. Wszystko to ostatecznie ma zapewnić ciągłość działania i minimalizację skutków potencjalnych incydentów.

Zabezpieczenie – praktyki, procedury i mechanizmy, które mogą chronić przed zagrożeniem, minimalizować podatność, wykrywać niepożądane zdarzenia etc.

System zarządzania bezpieczeństwem informacji według standardu ISO

Jeszcze do niedawna jedną z głównych przesłanek wdrożenia systemu zarządzania bezpieczeństwem informacji, zgodnego ze standardami ISO, była chęć „podbicia" swojej pozycji rynkowej i wzrost konkurencyjności wobec firm substytucyjnych. Dla innych był to warunek konieczny do wzięcia udziału w ważnym przetargu czy zawarcia umowy. Obecnie, wraz z rozwojem technologii, wszechobecną cyfryzacją i przeniesieniem życia do sieci zapewnienie bezpieczeństwa informacji, poprzez systemowe nim zarządzanie, staje się niejako standardem i dobrą praktyką. Przestajemy robić coś, bo wymagają tego od nas inni, a zaczynamy świadomie decydować się na włączenie zarządzania bezpieczeństwem informacji w zakres działań operacyjnych.

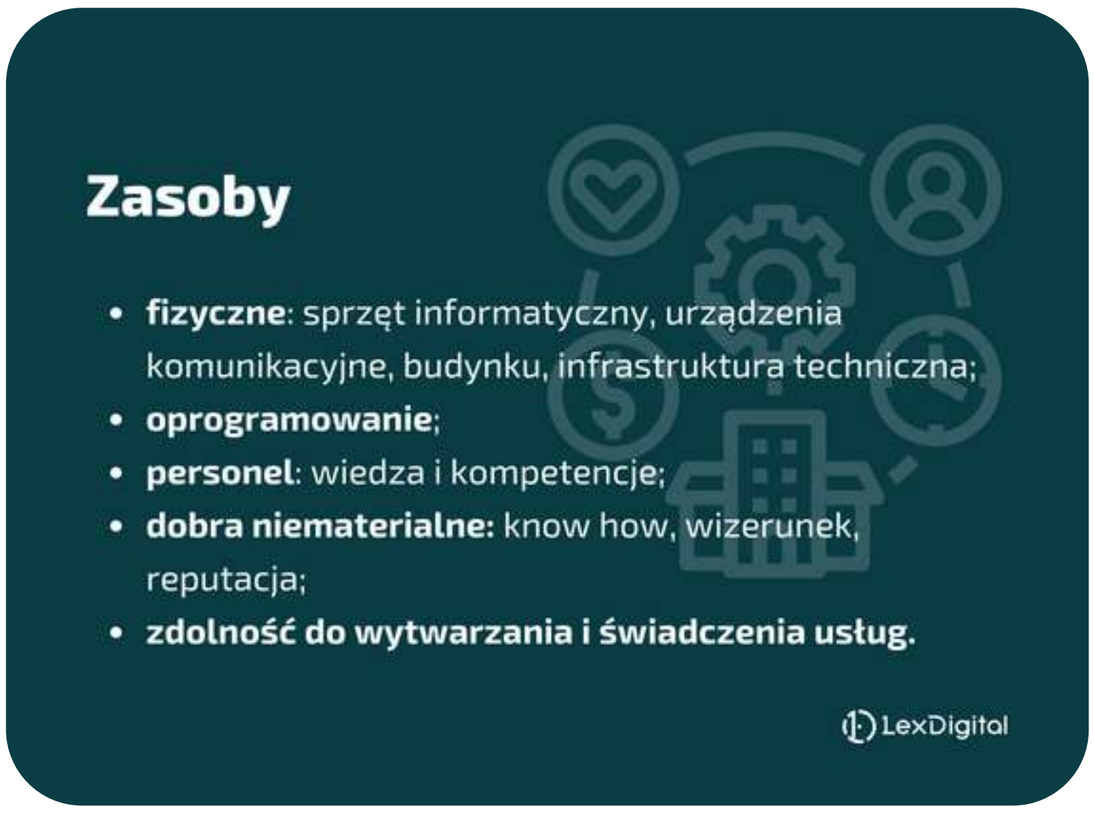
Z naszych obserwacji wynika, że na rynku jest wiele organizacji, które chciałyby wdrożyć wymagania standardu ISO/IEC 27001. Duża część jednak nie wie, jak zorganizować ten projekt, od czego zacząć, nie ma w swoich zespołach osób kompetentnych w tym zakresie lub po prostu boi się zaangażowania swoje zasoby w projekt, który pozornie, zamiast dostarczać zysków, generuje koszty. Oczywiście pozornie, bo jeżeli jeszcze w pierwszych etapach, podczas wdrożenia odpowiednich rozwiązań będzie wymagane poniesienie kosztów, tak w dłuższej perspektywie systemowe podejście do bezpieczeństwa informacji może uchronić nas niejednokrotnie przed wydatkami związanymi np. z koniecznością zapłaty kar pieniężnych za wykroczenia i inne incydenty.

ISO/IEC 27001, jako integralna część procesów organizacji

Rozpoczynając przygodę z ISO/IEC 27001 musimy pamiętać o tym, że system zarządzania bezpieczeństwem informacji musi być częścią procesów funkcjonujących w organizacji oraz ogólnej struktury zarządzania i musi być z nimi zintegrowany. W praktyce oznacza to to, że wszystkie podejmowane działania w zakresie bezpieczeństwa informacji są adekwatne do naszych potrzeb i są niejako wpisane w realizowane procesy. Bezpieczeństwo informacji musi być także uwzględniane przy projektowaniu procesów, systemów informacyjnych oraz zabezpieczeń.

Dlaczego jest to tak ważne? Dlatego, że waga poszczególnych atrybutów bezpieczeństwa tj. poufności, integralności czy dostępności w każdej organizacji będzie różna. Przykładowo dla instytucji finansowych, w tym banków, szczególne znaczenie, rzutujące na ich renomę, ma poufność danych. Integralność danych to kluczowy aspekt między

innymi dla organizacji opracowujących różnego rodzaju badania statystyczne, gdyż błąd w tym obszarze może wpływać na ich wiarygodność. Zapewnienie dostępności jest natomiast priorytetem w przypadku małych organizacji, gdzie przerwa w działaniu systemu może doprowadzić do poważnych strat finansowych.



Podejście procesowe

Kolejnym ważnym elementem, na który na pewno warto zwrócić uwagę, jest podejście procesowe. Czyli nic innego jak myślenie o działaniach w kontekście przekształcania danych wejściowych w wyjściowe z zastosowaniem odpowiedniej sekwencji oddziałujących na siebie zadań. Takie podejście pozwala zachować oszczędność zasobów przy równoczesnym kompleksowym zarządzaniu całym systemem. W tym celu wykorzystać można tzw. cykl życia informacji, czyli okres od momentu wytworzenia informacji poprzez jej wykorzystanie, w tym przetwarzanie, przekazywanie, powielanie, przechowanie, po zniszczenie lub uszkodzenie. Prześledzenie przepływu informacji w organizacji od momentu jej wytworzenia po usunięcie pozwala uchwycić wszystkie aktywa, które mają styczność z tą informacją i tym samym minimalizować ryzyko błędu czy pominięcia.

Cała norma ISO/IEC 27001 oparta jest na koncepcji podejścia procesowego ściśle związanego z podejściem opartym na ryzyku. Dokonujemy analizy ryzyka, wdrażamy zaplanowane działania mitygujące, weryfikujemy ich skuteczność i modyfikujemy w myśli zasady ciągłego doskonalenia.

Każdy zasób w organizacji ma dla niej wartość, dlatego konieczne jest zagwarantowanie tym zasobom odpowiedniego stopnia ochrony. Ważne jest także to, żeby już na etapie wdrożenia systemu możliwie najdokładniej zidentyfikować wszystkie zasoby i określić ich rolę w organizacji i bezpieczeństwie informacji.

Kroki, które należy podjąć, aby skutecznie wdrożyć system zarządzania bezpieczeństwem zgodny z ISO/IEC 27001

1. Zaplanuj projekt

Dobry plan to podstawa. Na początku warto ustalić ramy czasowe projektu.Przyjmuje się, że optymalny czas wdrożenia systemu to od 6 do 10 miesięcy w zależności od rozmiarów organizacji, jej struktury zarządczej, skomplikowania i złożoności realizowanych procesów oraz dojrzałości informatycznej. Następni musimy wybrać lidera, który będzie koordynował wszystkimi pracami. Dobrze także zdecydować jakim budżetem dysponujemy oraz określić jakie inne zasoby mogą nam być potrzebne. To też dobry moment, żeby zastanowić się, czy działamy sami, czy decydujemy się na wsparcie podmiotów zewnętrznych.

2. Zorganizuj pracę

Organizację pracy warto rozpocząć od utworzenia zespołu odpowiedzialnego za wdrożenie wymagań standardu. Jego członkowie powinni w kolejności ustalić zasady współpracy oraz wybrać metodykę wdrażania systemu zarządzania bezpieczeństwem informacji.Norma ISO/IEC 27001 zaleca, aby przyjąć podejście procesowe oraz podejście oparte na ryzyku. Biorąc pod uwagę złożoność projektu, dobrze przygotować sobie harmonogram realizacji poszczególnych zadań, co ułatwi nam sprawowanie kontroli nad projektem, czy nawet wcześniejsze zaplanowanie spotkań z pracownikami.

3. Wdrażaj krok po kroku rozwiązania, spełniające kolejne wymagania standardu

Norma wraz z załącznikiem A jest bardzo dobrym drogowskazem do planowania i realizacji poszczególnych zadań. Traktując ją jako przewodnik, podejmij następujące kroki.

- **Określenie kontekstu organizacji** – to nic innego jak zdefiniowanie czynników wewnętrznych i zewnętrznych, które oddziałują na organizację i mogą mieć znaczenie dla zachowania bezpieczeństwa informacji, w tym m.in. przepisy prawa, dostępne technologii, uregulowania kulturowe, kultura organizacji; inaczej to po prostu opis środowiska, w którym funkcjonuje organizacja i w którym realizuje swoje cele.

- **Zdefiniowanie aktywów** – stworzenie rejestru wszelkich urządzeń, oprogramowania i innych elementów infrastruktury, które mają znaczenie dla organizacji i wpływają na bezpieczeństwo informacji; zdefiniowanie aktywów to kluczowy etap procesu wdrażania, bez którego praktycznie niemożliwe jest przystąpienie do kolejnych kroków.

- **Zarządzanie ryzykiem** – owiany złą sławą proces, który dobrze przeprowadzony może być doskonałym narzędziem dla realizacji kolejnych prac. Punktem wyjścia jest ustanowienie dopasowanej do organizacji metodyki szacowania ryzyka, a następnie zdefiniowanie ryzyk w odniesieniu do każdego aktywa, które zinwentaryzowaliśmy. Ryzyka mogą wynikać z zagrożeń związanych z czynnikami fizycznymi, ludzkimi oraz technologicznymi i w szczególności odnoszą się do utraty atrybutów bezpieczeństwa tj. poufności, dostępności i integralności informacji. Norma zaleca, aby w czasie szacowania ryzyka uwzględniać identyfikowanie, obliczanie i nadawanie priorytetów poszczególnym ryzykom. Rezultaty analizy pozwalały natomiast pozwolić na określenie właściwych działań zarządczych.

- **Plan postępowania z ryzykiem** – ryzyka zdefiniowane w poprzednim etapie pojawiają się z różnym prawdopodobieństwem oraz niosą różne skutki, dlatego istotne jest zaplanowanie działań, które pozwolą nam zarządzać tym ryzykiem, w tym zminimalizować ich wpływ na skuteczność naszego systemu. Możemy to w szczególności osiągnąć przez:
  - zastosowanie odpowiednich zabezpieczeń w celu redukcji ryzyka,
  - świadomą i obiektywną akceptację ryzyka, pod warunkiem, że w sposób satysfakcjonujący spełnia politykę organizacji i kryteria akceptacji ryzyka,
  - unikanie ryzyka, nie zezwalając na działania, które mogłyby spowodować jego wystąpienie,
  - podzielenie się odpowiednim ryzykiem z innymi podmiotami, np. ubezpieczycielami, dostawcami.

- **Wybór i wdrożenie odpowiednich zabezpieczeń** – podejmowanie konkretnych działań, które będą służyć minimalizacji ryzyka, które zdefiniowaliśmy i oszacowaliśmy we wcześniejszych etapach projektu. Wybierając odpowiednie rozwiązania, należy zwrócić uwagę na:
  - przepisy prawa i inne regulacje, które odnoszą się do przedmiotu i miejsca naszej działalności,
  - cela organizacji,
  - wymagania i ograniczenia eksploatacyjne tych rozwiązań,
  - koszty wdrożenia i eksploatacji, aby były proporcjonalne do ryzyk – m.in. wybieramy rozwiązania, które pozwolą nam minimalizować zdefiniowane ryzyka w najszerszym możliwym zakresie,
  - rzeczywiste potrzeby ich wdrożenia; stosowanie nadmiarowych środków może przynieść odwrotne skutki, np. zbyt restrykcyjne zasady, nieadekwatne do problemu mogą spotkać się z oporem ze strony pracowników, eksploatacji takich rozwiązań może także przewyższać materialnie skutki danego ryzyka;

Zaleca się, aby w późniejszych etapach, kiedy utrzymujemy już wdrożony system, środki bezpieczeństwa rozpatrywane były już na etapie projektowania, ponieważ nieuwzględnienie tego może spowodować dodatkowe koszty, mniejszą skuteczność a w najgorszym razie nawet nieosiągnięcie określonych celów bezpieczeństwa.

Zabezpieczenia możemy podzielić na następujące kategorie:

- organizacyjne: są to wszelkiego rodzaju polityki, procedury, instrukcje, regulaminy, oświadczenia, które regulują zasady postępowania w wybranych obszarze działalności organizacji, to także umowy z kontrahentami i dostawcami, które uwzględniają zasady bezpieczeństwa informacji, etc;

- fizyczne: wszystko to, co pozwala nam zachować bezpieczeństwo dla naszych aktywów, w tym np. kontrola dostępu do pomieszczeń, alarmy przeciwwłamaniowe, gaśnice i inne systemu wykrywające zagrożenie ogniem, czujniki dymu, monitoring wizyjny, etc;
- techniczne/ informatyczne: zabezpieczenia stosowane w zasobach informatycznych, w tym kopie zapasowe, zarządzanie uprawnieniami, testy penetracyjne, ochrona antywirusowa i kryptografia, testowanie zabezpieczeń, monitorowanie nietypowych zdarzeń (zbieranie i kontrola logów), etc.

4. Szkól i uświadamiaj pracowników

Kiedy zidentyfikowaliśmy już ryzyka zagrażające bezpieczeństwu informacji i ustanowiliśmy zabezpieczenia pomagające nam w ich minimalizacji, przyszedł czas na uświadamianie naszych pracowników. Szkolenia mają z jednej strony wskazać, czego wymagamy od nich w zakresie bezpieczeństwa informacji, a z drugiej pokazać cele i korzyści systemowego podejścia do kwestii bezpieczeństwa. Pracownik, który zrozumie sens działań, z większym prawdopodobieństwem będzie się do nich stosowała.

Szkolenia powinny być dostosowane do danej grupy odbiorców jak najbardziej konkretne, pokazujące praktyczne przykłady. Zwracajmy uwagę na potencjalne konsekwencje, ale też nie straszymy nadmiernie pracowników, szukajmy pozytywnych argumentów.

5. Dokonaj wewnętrznej oceny systemu podczas audytu wewnętrznego i przeglądu zarządzania

Są to dwa obowiązkowe elementy, których wymaga od nas norma, a które służą ciągłemu doskonaleniu naszego systemu zarządzania bezpieczeństwem informacji.

Audyt to nic innego jak przegląd całej organizacji w odniesieniu do wymagań, które stawia nam norma. Szukajmy słabych elementów systemu, aby móc go doskonalić, zwracajmy jednak także uwagę na pozytywy, aby zachęcić pracowników do ciągłego respektowania wdrożonych zasad. Pamiętajmy także, że audyt wewnętrzny ma służyć nam, więc nie bójmy się definiować potencjałów do doskonalenia czy rekomendacji. Na pewno będzie to mile widziane podczas audytu certyfikującego.

Przegląd zarządzania to natomiast fachowa nazwa dla cyklicznych spotkań kadry zarządczej z osobami odpowiedzialnymi za utrzymanie systemu zarządzania bezpieczeństwem informacji. W trakcie takich spotkań omawiane są najistotniejsze obszary tegoż systemu, w tym m.in. wyniki szacowania ryzyka, stan wdrożonych zabezpieczeń, wyniki ostatnich audytów czy status zagospodarowania rekomendacji. Przegląd zarządzania ma też na celu włączenie i aktywizację szczebla zarządczego w organizacji, który powinien stanowić przykład dla pracowników niższych szczebli.

Zarówno z przeglądu zarządzania, jak i audytu dobrze jest przygotować raport lub chociaż notatkę z wyszczególnionymi ustaleniami.

6. Poddaj się audytowi certyfikującemu

Zwieńczeniem wielomiesięcznych prac jest przystąpienie do audytu prowadzonego przez niezależną jednostkę certyfikującą, która podobnie jak na audycie wewnętrznym krok po kroku zweryfikuje zgodność z wymaganiami normy na podstawie przedstawionych przez organizację dowodów.

Czas trwania audytu jest uzależniony od wielkości organizacji, złożoności procesów, ilości lokalizacji i najczęściej zajmuje od 2 do 5 dni roboczych.

Pamiętaj, że sam* wybierasz jednostkę, która będzie prowadzić audyt. Współpracuj z audytorem, dyskutuj. Audyt to nie kontrola, dlatego potraktuj go jak element doskonalący Twój system. Rekomendacja czy nawet mała niezgodność nie dyskwalifikują Cię w staraniach o certyfikat.

Czynniki krytyczne sukcesu systemu zarządzania bezpieczeństwem informacji

Tyle ile jest organizacji, tyle może być czynników krytycznych, które będą wywierać bezpośredni lub pośredni wpływ na sukces wdrożenia systemu zarządzania bezpieczeństwem informacji. Niemniej warto zwrócić uwagę na kilka kwestii:

1. ustanowienie wewnętrznej polityki bezpieczeństwa dostosowanej do kultury organizacyjnej oraz wyznaczenie celi, jakim ma służyć system i pod nie określać dopiero poszczególne działania,
2. zasady i podejście do projektowania, wdrożenia, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji,
3. widoczne zaangażowanie i wsparcie kierownictwa na wszystkich szczeblach,
4. rzetelne podejście do zarządzania ryzykiem,
5. budowanie świadomości pracowników, ale również ich motywowanie, aby postępowali zgodnie z przyjętymi zasadami,
6. wdrożenie efektywnego procesu zarządzania incydentami,
7. opracowanie mechanizmów pozwalających na pomiar efektywności wdrożonych zasad i otwartość na sugestie stron zainteresowanych.

Podsumowując

Najważniejsze w całym procesie wdrożenia, a następnie utrzymania systemu zarządzania bezpieczeństwem informacji jest Twoje nastawienie. Otwartość na zmiany, nowe rozwiązania, a w końcu wiara w użyteczność tego, co robisz, jest kluczem do sukcesu. Warto również zadbać o zbudowanie systemu szytego na miarę Twojej organizacji. To, co sprawdza się u jednych, niekoniecznie będzie dobre dla Ciebie. Tylko system dopasowany do potrzeb organizacji, jej zasobów i możliwości będzie żył i przynosił oczekiwane korzyści.

Prasówka

NSA potwierdza stanowisko UODO: Bisnode karana za brak informacji o przetwarzaniu danych

Naczelny Sąd Administracyjny (NSA) potwierdził decyzję Urzędu Ochrony Danych Osobowych (UODO) dotyczącą nałożenia kary na spółkę Bisnode (obecnie Dun & Bradstreet) z powodu braku informacji dla osób, których dane przetwarzała.

Sprawa ta, trwająca ponad cztery lata, ma swoje źródło w nałożeniu kary na spółkę w wysokości ponad 943 tys. zł za brak informacji dla osób, których dane były przetwarzane. Przez brak tej informacji, te osoby nie były świadome przetwarzania ich danych osobowych, co uniemożliwiało im korzystanie z przysługujących im praw związanych z ochroną danych osobowych.

NSA potwierdził stanowisko UODO, które stwierdziło, że spółka Bisnode, pozyskując dane

z ogólnodostępnych rejestrów publicznych, zobowiązana była do przekazania informacji osobom, których dane te dotyczą, zgodnie z art. 14 RODO.

Spór ten wywołał kontrowersje, jednak NSA podkreślił, że zasada transparentności przetwarzania danych jest kluczowa w świetle RODO, a wszelkie wyjątki od tej zasady, takie jak "niewspółmiernie duży wysiłek," powinny być interpretowane ograniczająco.

Obecnie Prezes UODO będzie ponownie rozpatrywał sprawę w kontekście przetwarzania danych osób prowadzących w przeszłości działalność gospodarczą oraz wysokości nałożonej kary administracyjnej.

Źródło: Decyzja UODO

Jeśli masz nowy samochód, to jest to danoosobowy koszmar. Raport Mozilla wprowadza w szok

Nowy raport Privacy Not Included stowarzyszenia Mozilla rzuca światło na alarmujący stan prywatności w nowoczesnych samochodach. Według raportu, każda z 25 badanych marek samochodów, w tym takie jak BMW, Ford, Toyota, Tesla i Subaru, nie spełnia podstawowych standardów prywatności i bezpieczeństwa w nowych, internetowo połączonych modelach.

Mozilla znalazła dowody na to, że marki takie jak BMW, Ford, Toyota, Tesla i Subaru zbierają dane dotyczące kierowców, w tym informacje o rasie, mimice twarzy, wadze, informacje zdrowotne i miejsca, do których się udają. Niektóre z testowanych samochodów zbierały dane, których nie spodziewalibyście się, włączając w to szczegóły dotyczące aktywności seksualnej, pochodzenia etnicznego i statusu imigracyjnego. Producenci również zbierają dane za pomocą swoich aplikacji i stron internetowych, a następnie mogą je sprzedawać lub udostępniać osobom trzecim.

Raport zauważa także, że wiele marek stosuje "pranie wizerunku", czyli przedstawia konsumentom informacje sugerujące, że nie muszą się martwić o prywatność, podczas gdy jest inaczej. Dodatkowo, wiele marek wciąż stawia na zawiłe i trudne do zrozumienia polityki prywatności, co utrudnia kierowcom zrozumienie, jakie dane są zbierane.

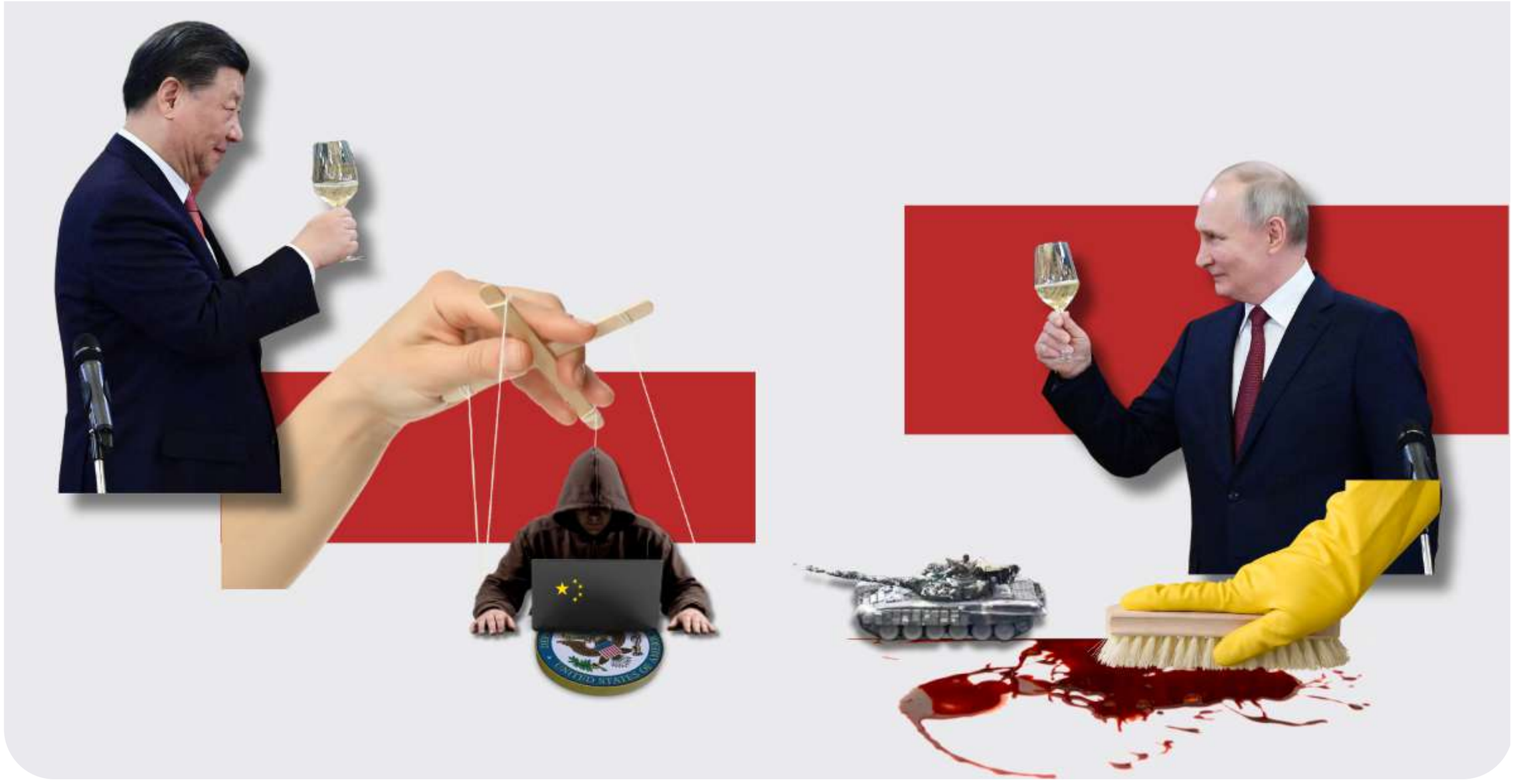
Pytania dotyczące zgody również są zasadniczo żartem. Na przykład Subaru mówi, że będąc pasażerem w samochodzie, jesteś uważany za "użytkownika", który wyraził zgodę firmy na zbieranie informacji o Tobie. Mozilla stwierdziła, że wiele marek samochodów twierdzi, że to odpowiedzialność kierowcy informowanie pasażerów o polityce prywatności swojego samochodu – tak jakby te polityki prywatności były zrozumiałe dla kierowców w pierwszej kolejności. Na przykład Toyota ma konstelację 12 różnych polityk prywatności dla przyjemności czytania.

Źródło: Raport Privacy Not Included

IBM obiecywał wycofać się z rozpoznawania twarzy. Teraz podpisano kontrakt o wartości 69,8 miliona dolarów na rozwój technologii

IBM powraca na rynek rozpoznawania twarzy, mimo wcześniejszych zapewnień o zaniechaniu prac nad tą technologią z powodu obaw związanych z naruszeniami praw człowieka. Firma podpisała umowę o wartości 69,8 miliona dolarów z brytyjskim rządem na rozwój platformy biometrycznej, która będzie oferować funkcję rozpoznawania twarzy dla służb imigracyjnych i organów ścigania. Pomimo wcześniejszych zapewnień, umowa ta budzi kontrowersje w kontekście naruszeń prywatności i praw człowieka. IBM zaprzecza, twierdząc że nie wspiera masowego nadzoru i naruszeń praw człowieka, ale obrońcy praw człowieka mają inne zdanie.

Źródło: Śledztwo The Verge



Chińscy hakerzy odpowiedzialni za włamanie się do Departamentu Stanu USA

Co najmniej 60 000 e-maili zostało skradzionych z Departamentu Stanu USA po włamaniu chińskich hakerów do usługi poczty e-mail Microsoft Exchange.

Urzędnicy Departamentu Stanu ogłosili w trakcie briefingu dla personelu Senatu, że w maju dziesiątki tysięcy e-maili zostały zhakowane. Listy pochodziły z 10 kont departamentu, z czego dziewięć znajdowało się w Azji Wschodniej i na Pacyfiku, a jedno w Europie.

Hakerzy mieli dostęp do kont e-mailowych 25 organizacji od maja, w tym do departamentów stanu i handlu USA, ale fakt włamania został ujawniony w tym miesiącu przez rzecznika Departamentu Stanu, Matthewa Millera.

Atak przypisuje się chińskiej grupie o nazwie Storm-0558. Departament Stanu USA nie dokonał jeszcze konkretnej atrybucji, ale zgadza się z podejrzeniami Microsoftu odnośnie zaangażowania Storm-0558 w atak.

"W tym momencie nie dokonaliśmy atrybucji, ale, jak powiedziałem wcześniej, nie mamy powodu wątpić w atrybucję, którą Microsoft podał publicznie" – mówi Miller. "Był to włamanie do systemów Microsoft, które Departament Stanu odkrył i powiadomił Microsoft."

Źródło: https://bit.ly/45mbuCQ

Wzrost rosyjskich cyberataków. Celem są państwowe organy ścigania

Rosyjscy szpiedzy atakują systemy komputerowe agencji ścigania Ukrainy, próbując zidentyfikować i zdobyć dowody związane z rosyjskimi zbrodniami wojennymi. Ataki celują w Prokuraturę Generalną Ukrainy i działy dokumentujące zbrodnie wojenne, powiedział Yurii Shchyhol, szef Państwowej Służby Specjalnej Komunikacji i Ochrony Informacji Ukrainy (SSSCIP). Liczba incydentów związanych z bezpieczeństwem cybernetycznym udokumentowanych przez SSSCIP wzrosła o 123% w pierwszej połowie 2023 w porównaniu z drugą połową 2022 roku.

Hakerzy próbowali także zdobywać informacje wywiadowcze o rosyjskich obywatelach aresztowanych w Ukrainie, aby "pomóc tym osobom uniknąć ścigania i przenieść je z powrotem do Rosji". Rosjanie priorytetowo koncentrują się na atakowaniu organów rządowych i próbie dostania się do ich serwerów pocztowych.

19.09.2023 Międzynarodowy Trybunał Karny z siedzibą w Holandii (ICC) wykrył "niezwykłą aktywność" w swojej sieci komputerowej. Nadal nie jest jasne, kto stał za włamaniem. W marcu ICC wydał nakaz aresztowania Władimira Putina pod zarzutem nielegalnej deportacji dzieci z Ukrainy. Kreml odrzuca oskarżenia i jurysdykcję sądu.

Źródło: https://reut.rs/46uAatJ

Polska

Brak świeżych kar z Polski. Gratulację dla wszystkich, dbających o ochronę danych osobowych!

Świat

Austriacki organ ochrony danych nakazał administratorowi dostosowanie banera plików cookie do art. 7 RODO i poinformowanie dostawców zewnętrznych o usunięciu danych osobowych skarżącego zgodnie z art. 19 RODO. Austriacki Urząd Ochrony Danych uznał, że firma Hearst Magazine Media, Inc. naruszyła RODO poprzez wyświetlenie na swojej stronie internetowej banneru cookie bez opcji "odmów", co uniemożliwiło jednoznaczną zgodę użytkownika na przetwarzanie danych. Skarżący zażądał usunięcia swoich danych, co Urząd Ochrony Danych uznał za słuszne, jednak dane te zostały już wcześniej usunięte. Kontroler został zobowiązany do poinformowania dostawców zewnętrznych o usunięciu danych.

Urząd Ochrony Danych stwierdził również, że obecna wersja banneru cookie nie spełnia wymogów art. 7 RODO i nakazał jego dostosowanie w ciągu 8 tygodni. W związku z brakiem obecnie trwającego nielegalnego przetwarzania danych, Urząd Ochrony Danych nie wydał decyzji nakazującej zaprzestanie przetwarzania danych.

Źródło: https://bit.ly/3PBaiFH

Fiński organ ochrony danych nałożył grzywnę w wysokości 23 000 euro na internetowy katalog przedsiębiorstw, ponieważ ten nie przestrzegał prawa osób, których dane dotyczą. W latach od 8 marca 2019 do 2 września 2022 roku Biuro fińskiego Rzecznika Ochrony Danych (DPA) otrzymało wiele skarg dotyczących Fińskiego Rejestru Firm, usługi wyszukiwania firm świadczonej przez Suomen Avainsanat Oy. Osoby, których dane były przetwarzane, skarżyły się na brak pełnego dostępu do nagrań rozmów oraz na konieczność składania pisemnych wniosków i dostarczania kopii dokumentów tożsamości w celu uzyskania swoich danych. DPA uznał, że działania firmy naruszyły prawa tych osób wynikające z przepisów RODO.

Konkretnie chodziło o prawo dostępu do danych oraz prawo do otrzymania kopii przetwarzanych informacji, zgodnie z art.12 ust.1 i art.15 ust.3 RODO. Firma dostarczyła jedynie ogólny opis rozmowy telefonicznej, nie wskazując, jakie dokładnie dane były przetwarzane.

W trakcie dochodzenia ex officio, DPA uznał również, że firma naruszyła przepisy dotyczące ułatwiania wykonywania praw osób, których dane były przetwarzane, oraz weryfikacji ich tożsamości (art.12 ust.6 i art.12 ust.2 RODO). Firma nie pozwalała na elektroniczne składanie wniosków o dostęp do danych, choć przetwarzanie danych odbywało się drogą elektroniczną. Dodatkowo, żądała od osób, których dane dotyczyły, dostarczenia pisemnych wniosków i kopii dokumentów tożsamości, co było nieuzasadnione.

Organ ochrony danych nałożył na administratora grzywnę w wysokości 23 000 EUR na podstawie art. 58 ust. 2 lit.i) RODO i art. 83 ust. 6 RODO, ponieważ administrator nie podał informacji o swoich obrotach w 2022 r., a sankcję oszacowano na podstawie potwierdzonych obrotów w 2021 r.

Źródło: https://bit.ly/3PHKs2K

Hiszpański organ ochrony danych nałożył na másLUZ Energía (SIE) grzywnę w wysokości 70 000 euro za naruszenie art.6 ust.1 RODO czyli niezgodnie z prawem przetwarzanie danych osobowych po anulowaniu umowy na dostawy energii i gazu. Osoba, której dane dotyczą omyłkowo podpisała umowę z másLUZ Energia za pośrednictwem wiadomości SMS. Jednak, kiedy zdała sprawę, że SIE udaje własnego dostawcę energii skarżącego, zażądała anulowania umowy. Niemniej jednak administrator nadal wystawiał osobie, której dane dotyczą, faktury zużycia energii, które były automatycznie opłacane za pośrednictwem jej konta bankowego. Ponadto w styczniu 2022 r. administrator ponownie zmienił umowę o energię elektryczną bez zgody osoby, której dane dotyczą.

Źródło: https://bit.ly/3EXiKu7

Słoweński organ ochrony danych nakazał administratorowi zaprzestanie używania niektórych kamer wideo na terenie firmy, ponieważ monitoring wideo m.in. toalet i korytarzy, nie może opierać się na uzasadnionym interesie, gdyż nie istnieje realne zagrożenie dla mienia i ludzi.

Administrator nalegal, że przeprowadzenie monitoringu nie było możliwe w mniej restrykcyjny sposób. Dodatkowo wprowadzono środki zabezpieczające: dostęp do archiwum nagrań wideo był chroniony hasłem, ograniczony do określonych osób i dostępny tylko w wyjątkowych przypadkach, np. w celu dostarczenia dowodów w postępowaniach karnych. Administrator poinformował związek zawodowy i przedstawił powody instalacji kamer, które zostały poparte przez związek.

Informacja dla pracowników o instalacji systemu onitoringu wideo, była umieszczona na tablicy ogłoszeń firmy. Administrator uważał, że monitoring był zgodny z przepisami dotyczącymi monitoringu wideo, mógł być oparty na art. 6 ust. 1 lit. f RODO oraz spełniał wymogi artykułów 3, 24 i 74 ZVOP-1 oraz artykułu 38 konstytucji słoweńskiej.

DPA natomiast uznał, że monitorowanie całego obszaru nie było zgodne z przepisami i RODO, ponieważ można było to zrobić w mniej restrykcyjny sposób. Stwierdził także, że firma nie spełniła warunków uzasadnionego interesu, nie przeprowadzając odpowiedniego testu wyważania. Ponadto monitorowanie w niektórych miejscach, takich jak toalety, było nieproporcjonalne i naruszało prywatność pracowników. W rezultacie firma musiała dostosować swoje praktyki monitorowania do wymogów prawa i RODO.

Źródło: https://bit.ly/3LKm1kh

Dziękujemy za przeczytanie Naszego Newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI