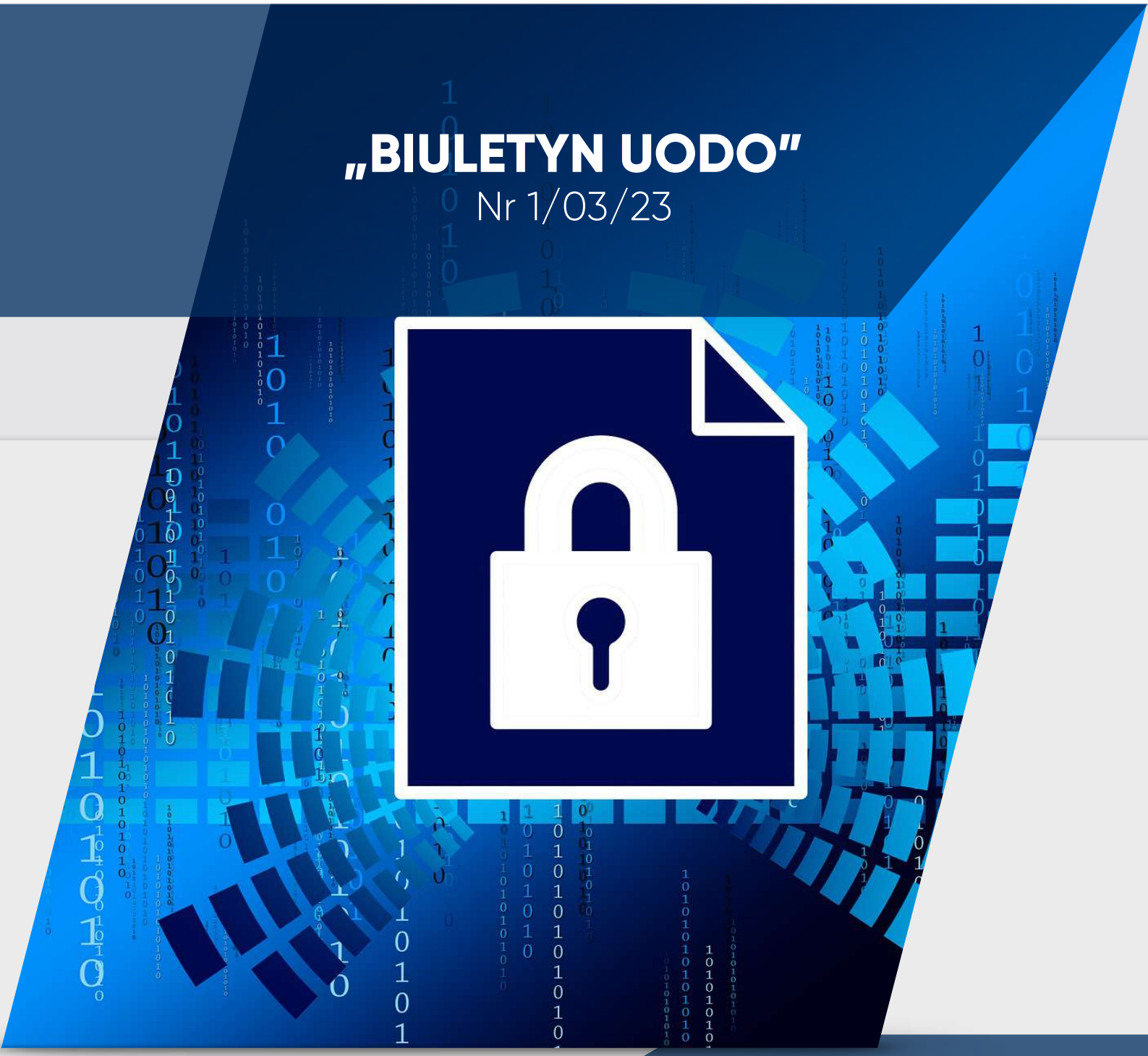
URZĄD OCHRONY DANYCH OSOBOWYCH

„BIULETYN UODO"

Nr 1/03/23



www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo, Drodzy Czytelnicy!

Pragnę Państwa przywitać i serdecznie zachęcam do zapoznania się z nową formułą naszego miesięcznika. Mam nadzieję, że rozbudowany i bogatszy w treść „Biuletyn UODO" przypadnie Państwu do gustu. Za nami 25 lat systemu ochrony danych osobowych w Polsce i prawie 5 lat stosowania RODO. Liczby te potwierdzają, że ochrona danych osobowych i prawo do prywatności towarzyszą nam już dość długo. W otaczającym nas świecie następuje jednak wiele zmian, do których my – obywatele, administratorzy, inspektorzy ochrony danych – musimy się dostosować. Widząc jak w ostatnich latach dynamicznie zmienia się otaczająca nas rzeczywistość, np. poprzez przyspieszenie cyfryzacji, widzimy jak ważna jest nieustanna dbałość o ochronę danych osobowych i bieżące reagowanie na zachodzące zmiany.

RODO to niekończący się proces, nieustannie wymagający dostosowywania przyjętych rozwiązań do zmieniających się warunków. I choć przepisy RODO nie zmieniły w sposób rewolucyjny przepisów dotyczących ochrony danych osobowych, to w praktyce ochrona danych osobowych może być wyzwaniem, nie mamy co do tego wątpliwości. Z doświadczenia organu nadzorczego wynika, że już nawet samo rozumienie definicji wymienionych w RODO, choćby tego czym są dane osobowe może wprowadzać problemy interpretacyjne. UODO nieustannie podejmuje działania, aby takie wątpliwości rozwiewać. Urząd angażuje się w krajową legislację, poprzez opiniowanie przekazywanych do konsultacji projektów aktów prawnych. Ponadto UODO na bieżąco śledzi orzecznictwo w zakresie ochrony danych osobowych. Widzimy, że w wielu sprawach sądy podzielają stanowiska Urzędu wyrażane w decyzjach administracyjnych. Jednakże, odnotowujemy, że niestety zdarzają się różne podejścia interpretacyjne odnoszące się do faktu uznania danych osobowych m.in. dotyczące spraw związanych z numerem telefonu czy numerem rejestracyjnym pojazdu, czy do przetwarzania danych osobowych po zakończeniu dokonywania oceny zdolności kredytowej. Temat różnic interpretacyjnych jest na tyle istotny, że ma realny wpływ na ochronę danych osobowych i prawa do prywatności każdego obywatela. Dlatego też Urząd Ochrony Danych Osobowych już 31 marca 2023 r. organizuje konferencję „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów". Jestem przekonany, że wydarzenie to, które organizowane jest we współpracy z Akademią Ekonomiczno-Humanistyczną w Warszawie, przyczyni się do poważnej i merytorycznej dyskusji na temat prawa do ochrony danych osobowych i poszanowania prywatności w trosce o dobro każdego z nas. Szczegóły na temat konferencji są dostępne na naszej stronie **www.uodo.gov.pl**. Serdecznie na nią Państwa zapraszam.

Jakub Groszkowski
Zastępca Prezesa UODO

Szanowni Państwo, Drodzy Czytelnicy!

Witamy serdecznie na nowych łamach „Biuletynu UODO". Zmieniła się nie tylko nazwa, ale przede wszystkim formuła. Od teraz będziemy się starać dostarczać Państwu jeszcze więcej, mamy nadzieję, pożytecznych i interesujących treści.

Zauważyliśmy, że z roku na rok wzrastała liczba subskrybentów naszego periodyku. Obecnie, każdego miesiąca trafia on do ponad 9 tys. osób! Okazuje się, że czytają go nie tylko inspektorzy ochrony danych, dlatego będziemy się starać, aby prezentowane w nim materiały były jeszcze bardziej zróżnicowane.

Dlatego w „Biuletynie UODO" pojawi się więcej treści o charakterze problemowym i poradnikowym. Publikowane materiały będą odpowiedzią na najczęściej pojawiające się pytania i sygnały, jakie różnymi kanałami od Państwa otrzymujemy.

Marcowe wydanie biuletynu otwiera rozmowa z dr Urszulą Góral, jedną z tegorocznych laureatek Nagrody im. M. Serzyckiego.

Regularnie w UODO odnotowujemy wzrost zgłaszanych naruszeń ochrony danych osobowych. Dlatego polecam Państwa uwadze materiał na ten temat, który w jasny sposób wyjaśnia, na czym polega istota naruszenia. Sposobem na skuteczne przeciwdziałanie naruszeniom ochrony danych osobowych, które niosą za sobą wysokie ryzyko dla praw lub wolności osób fizycznych, są odpowiednie środki techniczne i organizacyjne. O tym, czy można do nich zaliczyć szyfrowanie przeczytacie Państwo w materiale zamieszczonym w sekcji „Nowe technologie".

W tym numerze podejmujemy także ważną z punktu widzenia obywateli sprawę udostępniania danych osobowych osób sygnalizujących nieprawidłowości. W wydanej decyzji UODO zajął jednoznaczne stanowisko, że udostępnianie danych osobowych osób sygnalizujących nie jest niezbędne dla prowadzenia postępowania administracyjnego. Co równie ważne, stanowisko to zostało potwierdzone w wyroku WSA, który oddalił skargę upomnianego podmiotu. Wyrok ten ma ogromne znaczenie w kontekście pewnych różnych podejść pojawiających się w orzecznictwie. Każdą taką sprawę analizujemy i reagujemy, korzystając z instrumentów, jakimi polski organ nadzorczy dysponuje.

Szczególnie polecam materiały, które będą pojawiać się w nowej sekcji: UODO sygnalizuje. Tu znajdziecie Państwo treści wypływające z analiz Departamentu Orzecznictwa i Legislacji. W tym numerze możemy przeczytać o tym, dlaczego sądy okręgowe powinny informować UODO o sprawach dotyczących roszczeń.

Na koniec zachęcam Państwa do zapoznania się z materiałami w sekcji poświęconej sprawom międzynarodowym, gdzie oprócz informacji o nakładanych karach przez inne organy nadzorcze, prezentujemy Państwu bardzo ważny wyrok TSUE o łączeniu funkcji inspektora ochrony danych. Jest to o tyle ważne, że wyrok ten potwierdza dotychczasowe stanowiska UODO wyrażane niejednokrotnie w tej sprawie.

Warto przy tej okazji nadmienić, że Biuletyn nie jest jedyną formą kontaktu z Państwem. Ponadto do dyspozycji osób fizycznych, administratorów i inspektorów pozostaje infolinia UODO, a także strona www. Jak pewnie Państwo zauważyliście od nowego roku zmieniliśmy także stronę www UODO.

Obecnie treść i warstwa graficzna nowej witryny, która działa pod dotychczasowym adresem www.uodo.gov.pl, jest dostosowana do naszych głównych grup docelowych z jasnym podziałem na sekcje: Dla Obywatela, Administratora i IOD-a. Dodatkowo wprowadzaliśmy także zakładkę: Załatw sprawę, aby wszyscy zainteresowani w szybki i przejrzysty sposób mogli dotrzeć do właściwych formularzy do kontaktu z UODO.

Warto także dodać, że UODO jako instytucja publiczna jest zobligowany do zapewnienia dostępności swoich stron internetowych zgodnie z ustawą z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych. Dołożyliśmy wielu starań, aby nowa witryna stała się dostępniejsza dla osób ze szczególnymi potrzebami.

Natomiast dla tych wszystkich, którzy bardzo przywiązali się do naszej poprzedniej witryny zostawiliśmy ją dostępną jeszcze w tym roku w formie archiwum pod adresem:

http://archiwum.uodo.gov.pl/

Zapraszam do lektury!

Adam Sanocki
Rzecznik Prasowy UODO
Dyrektor Departamentu
Komunikacji Społecznej UODO

DZIAŁANIA EDUKACYJNE WYMAGAJĄ KONTYNUACJI

Urszula Góral, inspektor ochrony danych w Kancelarii Sejmu, w rozmowie z Eweliną Janczylik-Foryś o potrzebie upowszechniania w społeczeństwie wiedzy o ryzyku, przepisach RODO, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych oraz rozumieniem tego zjawiska.

Jak odbiera Pani przyznanie nagrody im. Michała Serzyckiego?

Nagroda im. Michała Serzyckiego to najważniejsze wyróżnienie, które przyznawane jest przez polski organ ochrony danych osobowych. Dla mnie ma znaczenie symboliczne, bo zaczynałam pracę w Biurze GIODO właśnie za czasów ministra Michała Serzyckiego. Był to okres bardzo ciekawy w życiu organu ochrony danych. Po 10 latach funkcjonowania systemu ochrony danych osobowych w Polsce, organ był już dobrze rozpoznawalny w kraju, jak i za granicą. Wkład ministra Serzyckiego w budowę wizerunku GIODO był niezwykle istotny. Z jednej strony postawił na edukację, tu zwłaszcza na działania skierowane do szkół w ramach programu „Twoje dane – Twoja sprawa", z drugiej zaś otworzył organ na współpracę z wieloma środowiskami, zarówno z sektora prywatnego i publicznego. Ta forma szerokiej współpracy zaowocowała podpisaniem licznych porozumień o współpracy ze stowarzyszeniami i zrzeszeniami przedsiębiorców, jak również szkołami wyższymi, i ta współpraca często jest kontynuowana do dziś. Należy również podkreślić wkład M. Serzyckiego w ugruntowanie pozycji GIODO na forum międzynarodowym, czego szczególnym przejawem był wybór na stanowisko wiceprzewodniczącego Grupy Roboczej Art. 29. Ustanowienie tej nagrody to wyraz chęci upamiętnienia śp. Michała Serzyckiego, który zasługuje na zachowanie jego pamięci, w tym zwłaszcza zasług dla rozwoju polskiego organu ochrony danych. W całej 25-letniej historii polskiego organu ochrony danych, każdy jego szef wniósł doniosły wkład w jego działalność, kładąc różne akcenty na szereg jakże licznych zadań tej instytucji. Warto więc postrzegać obecne kierunki rozwoju Urzędu Ochrony Danych Osobowych, również mając w pamięci jego wcześniejsze dokonania.

Czy widzi Pani potrzebę dalszej edukacji w zakresie ochrony danych osobowych? Czy dostrzega Pani nowe obszary?

W obecnych czasach dużo mówi się o potrzebie edukacji, zwłaszcza edukacji cyfrowej. Nowoczesne technologie wymagają od wszystkich, aby korzystać z nich ze świadomością możliwości jakie daje ich zastosowanie, zarówno w codziennym życiu, jak i w usługach oferowanych tak przez biznes, jak i administrację publiczną. Działania edukacyjne skierowane do dzieci są szczególnie ważne, ponieważ wpływają na kształt i kondycję przyszłego pokolenia i społeczeństwa. Ale należy też otwarcie podkreślić, że te działania są również potrzebne nam dorosłym. Często nie mamy kontroli nad tym, co robią młodzi w Internecie, bo po prostu się na tym nie znamy. Dlatego należy uczulać, żeby nasza nadmierna pobłażliwość do nowinek i modnych trendów technologicznych nie wykluczyła nas z głównego kierunku w jakim rozwija się społeczeństwo i gospodarka.

Unijne organy ochrony danych mają tę cechę, że zajmując się materią niezwykle specyficzną lepiej widzą nadchodzące zjawiska i związane z nimi korzyści i zagrożenia. Dlatego głos organów ochrony danych w publicznej debacie na temat przyszłości edukacji w dobie cyfryzacji jest niezwykle istotny. Niestety często może zbyt mało słyszalny. W tym kontekście nagroda im. Michała Serzyckiego ma ten szczególny walor, że jest wyróżnieniem promującym wspólną ideę, a nie indywidualne autorytety. Bo z perspektywy ponad 15 lat pracy w tym obszarze widzę, jak niezwykle ważna jest umiejętność budowania kompromisów i wzajemnego wspierania się osób i łączenia środowisk zaangażowanych w działania na rzecz podnoszenia świadomości ochrony danych osobowych.

Z jakimi praktycznymi problemami spotyka się Pani na co dzień w swojej pracy?

Ochrona danych osobowych to temat, który nadal budzi wiele emocji i często obserwujemy skrajne podejście do samej regulacji prawnej jaką jest RODO. Od próby nadmiernego formalizowania i traktowania jako tzw. „wiedzy tajemnej" dostępnej tylko dla wybranego grona specjalistów, po ignorowanie i świadome pomijanie, często spowodowane brakiem wystarczającej wiedzy. Albo się zasady ochrony danych marginalizuje albo rozdmuchuje do gigantycznych rozmiarów przeszkód. Gdy po 15 latach pracy w UODO zdecydowałam się „sprawdzić" jako inspektor ochrony danych, zauważam, że również w tej roli mogę kontynuować działania mające na celu budowanie świadomości prawa do ochrony danych. W Polsce możemy pochwalić się całkiem pokaźnym dorobkiem, jeśli chodzi o funkcjonowanie tego jakże istotnego elementu całego systemu ochrony danych osobowych, jakim jest inspektor ochrony danych. Widzę tu jednak szereg dalszych wyzwań, zwłaszcza w zakresie prawidłowego postrzegania roli inspektora w organizacji. Używając analogii sportowej, porównałabym przepisy RODO do kijków do nordic walking – niby długie i nieporęczne, ale właściwie użyte pomagają w efekcie zapewnić prawidłową postawę i kondycję całego organizmu. Tak samo powinniśmy patrzeć na zapewnienie zgodności z zasadami ochrony danych w organizacji.

Jakie stoją wyzwania przed ochroną danych osobowych? Czy inne charakteryzują administrację publiczną, a inne sektor prywatny?

Jeśli chodzi o wyzwania w obszarze edukacji na temat prawa do prywatności i ochrony danych osobowych, to wierzę, że liczne grono wspaniałych i zaangażowanych nauczycieli i ekspertów, które przez lata zgromadził program UODO „Twoje dane – Twoja sprawa", przyniesie efekt kuli śniegowej i przyczyni się do jak najszerszego rozwoju kompetencji cyfrowych, zwłaszcza wśród dzieci i młodzieży. Niezwykle mnie cieszy, że wielu nauczycieli i ekspertów, z którymi współpracowaliśmy na przestrzeni lat w ramach programu TDTS, znajduje się co roku wśród 100 osób wyróżnianych przez Szerokie Porozumienie na rzecz Umiejętności Cyfrowych w Polsce. To oznacza, że działania edukacyjne są komplementarne, wspaniale się uzupełniają z korzyścią dla dzieci, młodzieży i wszystkich środowisk, do których są kierowane. To promocja wartości prawa do prywatności sama w sobie.

1 WYWIAD NUMERU / ROZMOWA Z EKSPERTEM

W tym roku mija 5 lat obowiązywania przepisów RODO. Nasze doświadczenia pokazują, że nadal zdarzają się przypadki nadinterpretacji przepisów, braku ich znajomości, nawet wśród urzędników czy przedsiębiorców. Potrzeba jest dalszych działań informacyjnych, tak aby wesprzeć administratorów w wyeliminowaniu różnych wątpliwości, jak np. wątpliwości związane z ustaleniem administratora, nadużywanie umów powierzenia przetwarzania danych osobowych czy problemy ze stosowaniem klauzul informacyjnych.

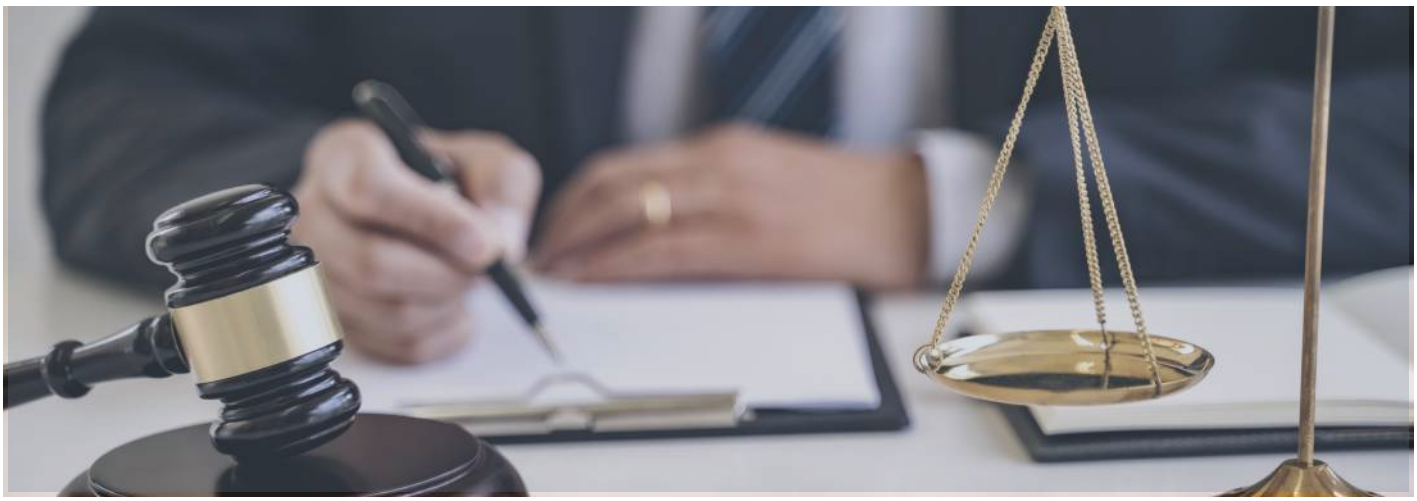
Tak więc, działania edukacyjne, które organ nadzorczy podejmował już za czasów min. Michała Serzyckiego, wydając poradniki dla przedsiębiorców czy pracodawców, ciągle wymagają kontynuacji, w tym np. aktualizacji praktycznych poradników i wskazówek. W mojej ocenie także ukształtowanie się roli IOD jest niezwykle ważne w budowie przyszłości skutecznego systemu ochrony danych, zwłaszcza, że UODO tak jak pozostałe organy europejskie, wspiera inspektorów w pełnieniu tej funkcji. IOD nosi na barkach często całą niechcianą w firmach czy instytucjach odpowiedzialność za stosowanie zasad ochrony danych osobowych. To dowód na to, że dalsza edukacja jest niezbędna, żeby zamienić obawy i niechęć przed „surowymi" zasadami RODO, w jasne i proste reguły, które porządkują rzeczywistość.

2 UODO SYGNALIZUJE

SĄDY OKRĘGOWE POWINNY INFORMOWAĆ ORGAN NADZORCZY O SPRAWACH DOTYCZĄCYCH ROSZCZEŃ

Sądy okręgowe powinny informować organ nadzorczy o wniesieniu pozwu oraz o prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, o którym mowa w art. 79 i 82 RODO.

Prawo osoby, której dane dotyczą, do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu zostało wprowadzone na podstawie art. 79 i art. 82 RODO i uszczegółowione z punktu widzenia procesowego w przepisach art. 92– 97 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Jak stanowi jej art. 92 w zakresie nieuregulowanym w RODO, do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i 82 RODO, stosuje się przepisy ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny.



Wzajemna wymiana informacji

W sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i 82 RODO, właściwy jest sąd okręgowy (o czym przesądza art. 93 ustawy o ochronie danych osobowych). Jego obowiązkiem jest (stosownie do art. 94 ust. 1 powołanej ustawy) niezwłoczne zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych o wniesieniu pozwu oraz o prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych. Zgodnie natomiast z art. 94 ust. 2 ustawy organ nadzorczy zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed Prezesem Urzędu Ochrony Danych Osobowych lub przed sądem administracyjnym, albo została zakończona. Prezes Urzędu Ochrony Danych Osobowych niezwłocznie informuje sąd również o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia.

2 UODO SYGNALIZUJE

Konsekwencje procesowe

Ustawa o ochronie danych osobowych przewiduje daleko idące konsekwencje procesowe dotyczące sytuacji, w której sąd oraz organ nadzorczy rozpatrują to samo roszczenie (skargę) o naruszenie przepisów o ochronie danych osobowych. Zgodnie bowiem z art. 95 ustawy o ochronie danych osobowych sąd zawiesza postępowanie, jeżeli sprawa dotycząca tego samego naruszenia przepisów o ochronie danych osobowych została wszczęta przed organem nadzorczym. Ponadto sąd okręgowy jest zobowiązany do umorzenia postępowania w zakresie, w jakim prawomocna decyzja organu nadzorczego o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocny wyrok wydany w wyniku wniesienia skargi, o której mowa w art. 145a § 3 4 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, uwzględnia roszczenie dochodzone przed sądem (art. 96 ustawy o ochronie danych osobowych). Co istotne, ustalenia prawomocnej decyzji organu nadzorczego o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi wiążą sąd okręgowy w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów (art. 97 ustawy o ochronie danych osobowych).

Ochrona praw osób

Należyte poinformowanie organu nadzorczego przez sąd o wniesieniu pozwu oraz o prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, ma zatem kluczowe znaczenie dla prowadzenia postępowania

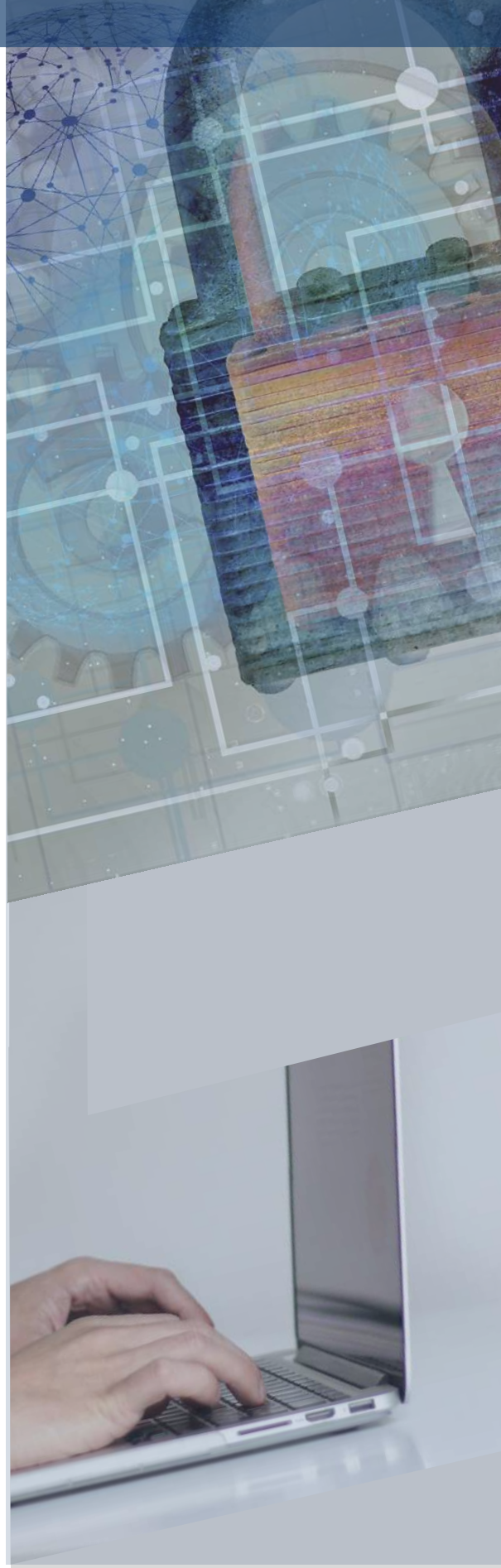
sądowego i prawidłowości wydanego wyroku. Prawidłowa realizacja przez sądy obowiązku nałożonego na nie mocą art. 94 ust. 1 ustawy o ochronie danych osobowych ma zapewnić równorzędny poziom gwarancji ochrony danych osobom, których dane dotyczą, w sprawach rozpatrywanych przed sądem powszechnym i organem nadzorczym i przede wszystkim sprzyjać wyeliminowaniu istotnej rozbieżności w ocenie prawnej stanów faktycznych w sprawach o podobne naruszenia rozpatrywanych przez te podmioty.

Jakich informacji oczekuje organ nadzorczy?

Ustawodawca nie precyzuje, co prawda, jakie informacje powinny zostać zawarte w przesyłanym organowi nadzorczemu zawiadomieniu o wniesieniu pozwu, jednak przyjmuje się, że ich zakres powinien co najmniej umożliwić identyfikację stron oraz wskazywać przedmiot postępowania, jak również datę wniesienia pozwu.

W odniesieniu zaś do orzeczeń kończących postępowanie w sprawie przyjmuje się, że powinna być chociażby przekazana data jego wydania, sentencja oraz informacja o dacie, z którą orzeczenie stało się prawomocne (por. Dmochowska A., Piotrowska A., Ustawa o ochronie danych osobowych. Komentarz, Wydawnictwo C.H.Beck 2018, s. 148).

Na kwestie te Prezes UODO wskazywał w wystąpieniu skierowanym w 2022 r. do Prezesów Sądów Apelacyjnych jako organów nadzorczych w stosunku do sądów okręgowych. Spotkało się ono z pozytywnym przyjęciem i zostało – zgodnie z prośbą – przesłane do sądów okręgowych. Zaowocowało to w pierwszym okresie wzrostem liczby zawiadomień kierowanych do Prezesa UODO, lecz w ostatnim czasie daje się zauważyć ich spadek. Dlatego warto po raz kolejny przypomnieć sądom okręgowym o ciążących na nich obowiązkach, tym ważniejszych, że od ich prawidłowej realizacji zależy realizacja gwarantowanych przez RODO praw osób, których dane zostały naruszone z powodu ich bezprawnego przetwarzania.



3 WYBRANE DECYZJE UODO

CZY MOŻNA UJAWNIAĆ DANE OSÓB ZGŁASZAJĄCYCH NIEPRAWIDŁOWOŚCI?

Urząd Ochrony Danych Osobowych udzielił upomnienia powiatowemu inspektorowi nadzoru budowlanego za naruszenie przepisów RODO polegające na udostępnieniu danych osobowych bez podstawy prawnej. WSA w Warszawie podtrzymał decyzję organu nadzorczego w tej sprawie.

Do Urzędu Ochrony Danych Osobowych wpłynęła skarga na nieprawidłowości w procesie przetwarzania danych osobowych przez powiatowego inspektora nadzoru budowlanego (dalej: powiatowy inspektor).

Na czym polegał problem?

Skarżąca zarzuciła powiatowemu organowi nadzoru budowlanego, że udostępnił osobom trzecim jej dane osobowe. Chodziło o dane zawarte w piśmie, w którym skarżąca poinformowała powiatowego inspektora o nieprawidłowościach w pracach budowlanych na działce sąsiadującej z jej nieruchomością, zaznaczając jednocześnie, że prosi o przeprowadzenie kontroli działań podejmowanych przez jej sąsiadów. W następstwie tego zgłoszenia powiatowy inspektor wszczął z urzędu postępowanie wyjaśniające w przedmiocie robót budowlanych, a wniosek skarżącej dołączył do akt postępowania. W postępowaniu przed organem ds. ochrony danych powiatowy inspektor wyjaśnił, że nie ujawnił osobom trzecim danych osobowych skarżącej, a jedynie stronom postępowania, dla których postępowanie to było jawne.

Jak rozwiązano problem?

W ocenie organu nadzorczego dane osobowe jednostki, która zawiadomiła go o potencjalnych nieprawidłowościach powinny zostać poufne w ramach postępowania prowadzonego przez ten organ z urzędu. Chodzi o sytuację, kiedy osoba ta nie jest stroną postępowania w sprawie toczącej się na skutek otrzymanego od niej zgłoszenia. W takim wypadku dane tej osoby nie mogą być ujawniane w toku postępowania stronom i uczestnikom tego postępowania.
Ponadto UODO przypomniał, że postępowania wszczynane z urzędu zgodnie z przepisami Kodeksu postępowania administracyjnego, wyposażają organ w instrumenty pozwalające na zbadanie sygnalizowanych przez obywateli nieprawidłowości, które może być przeprowadzone bez konieczności ujawniania źródła pozyskanych informacji.
Zdaniem Urzędu ujawnienie w aktach sprawy danych osobowych skarżącej, jako osoby zawiadamiającej o możliwych nieprawidłowościach, nie było niezbędne do przeprowadzonego postępowania, a więc do wypełnienia obowiązku prawnego ciążącego na powiatowym inspektorze, jako administratorze danych. Należy uznać, że udostępnienie to nastąpiło bez podstawy prawnej, a tym samym z naruszeniem art. 6 ust. 1 RODO.
Biorąc pod uwagę materiał dowodowy, UODO skorzystał w tej sprawie z instrumentu o charakterze naprawczym i w rezultacie udzielił powiatowemu inspektorowi upomnienia.
Decyzja Prezesa UODO* została zaskarżona przez powiatowego inspektora do Wojewódzkiego Sądu Administracyjnego w Warszawie. Jednak sąd administracyjny w wyroku z 2 lutego 2023 r.** skargę oddalił.

***DS.523.7153.2021**
****Sygn. akt II SA/Wa 1421/22**

4 NARUSZENIA I KONTROLE

CZYM JEST NARUSZENIE OCHRONY DANYCH OSOBOWYCH?

Złamanie przez pracownika procedur bezpiecznego przetwarzania danych, przypadkowa publikacja danych czy nieprawidłowa ich anonimizacja albo atak hakerski lub kradzież urządzenia elektronicznego zawierającego dane osobowe – to tylko przykładowe zdarzenia, których skutkiem może być naruszenie ochrony danych osobowych.

Wraz z wejściem w życie przepisów 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) administratorzy i podmioty przetwarzające stanęli przed koniecznością wywiązania się z szeregu obowiązków wynikających z tego aktu prawnego.

Kluczowy obowiązek administratorów

Wśród zadań spoczywających na administratorach wskazać można m.in. zgłaszanie występujących w ich organizacjach naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamianie o ich zaistnieniu osób, których dane dotyczą. W celu prawidłowego dostosowania się do panujących w tym obszarze regulacji niezbędnym staje się zatem zrozumienie oraz właściwe posługiwanie się pojęciem „naruszenia ochrony danych osobowych”.

Naruszenie ochrony danych, czyli co…

Zgodnie z definicją przedstawioną w art. 4 pkt 12 ogólnego rozporządzenia o ochronie danych „naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. W analogiczny sposób termin ten został określony przez ustawodawcę w art. 4 pkt 6 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125 z późn. zm.).

4 NARUSZENIA I KONTROLE

O „naruszeniu danych osobowych” mowa również w art. 174a ust. 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2022 r. poz. 1648), gdzie zostało ono zdefiniowane jako przypadkowe lub bezprawne zniszczenie, utrata, zmiana, nieuprawnione ujawnienie lub dostęp do danych osobowych przetwarzanych przez przedsiębiorcę telekomunikacyjnego w związku ze świadczeniem publicznie dostępnych usług telekomunikacyjnych.

Skutki naruszeń ochrony danych

Naruszenia ochrony danych osobowych przyjmują rozmaite formy. Mogą one zostać wywołane zarówno przez czynniki wewnętrzne, takie jak złamanie przez pracownika procedur bezpieczeństwa, przypadkowa publikacja danych czy nieprawidłowa ich anonimizacja, jak i zewnętrzne, takie jak atak hakerski lub kradzież urządzenia elektronicznego zawierającego dane. Skutki tego rodzaju incydentów mogą być bardzo poważne. Osoby, których dane dotyczą, stają się w ich rezultacie narażone na niebezpieczeństwa w postaci szkód majątkowych i niemajątkowych, a nawet uszczerbku fizycznego. Naruszenia ochrony danych osobowych mogą także prowadzić do poważnych konsekwencji dla samych administratorów. W tym kontekście niezwykle ważne jest, aby wszelkie podmioty przetwarzające dane osobowe działały zgodnie z przepisami dotyczącymi ochrony danych osobowych i stosowały odpowiednie środki bezpieczeństwa w celu zapobiegania ewentualnym naruszeniom. Firmy, które je lekceważą, ryzykują utratą zaufania klientów i partnerów biznesowych oraz narażają się na wysokie kary finansowe.

Naruszenia, które są zgłaszane Prezesowi UODO, często dotyczą następujących sytuacji:

- przesyłania dokumentacji administratora do osób nieuprawnionych (dotyczy to zarówno korespondencji e-mail, jak i korespondencji papierowej),
- zagubienia/kradzieży nośników elektronicznych/komputerów,
- nieprawidłowego niszczenia dokumentacji przez administratorów (częstym zjawiskiem jest sytuacja, gdy dokumentacja przeznaczona do zniszczenia nie jest niszczona w siedzibie administratora lub przy udziale profesjonalnej firmy, a odnajdywana jest po pewnym czasie przez osoby trzecie w miejscach publicznych lub na prywatnych posesjach),
- zagubienia dokumentacji papierowej przez administratora lub jego personel,
- ataków hakerskich skutkujących pozyskaniem lub/i zaszyfrowaniem baz danych administratora.

W 2022 administratorzy danych zgłosili do UODO blisko 12,7 tys. naruszeń ochrony danych osobowych. Te dane są bardzo zbliżone do tych z 2021 roku, gdy wszystkich zgłoszonych naruszeń było 12,9 tys.zł. Z tym, że dwa lata wcześniej naruszeń było około 7,5 tys.

5 NOWE TECHNOLOGIE

CZY SZYFROWANIE JEST SKUTECZNYM ZABEZPIECZENIEM PRZED UTRATĄ DANYCH?

Wraz z rozwojem nowych technologii, rośnie ilość przetwarzanych informacji, co determinuje wzrost ataków cybernetycznych. Z tego względu tak ważne jest zapewnienie ochrony danych za pomocą odpowiednich środków i form kryptografii, takich jak np. szyfrowanie, które pomogą zapobiegać naruszeniom danych i lepiej chronić organizację przed cyberatakami.

Mechanizm bezpieczeństwa w postaci szyfrowania danych jest wymieniony w art. 32 ogólnego rozporządzenia o ochronie danych (RODO) jako sposób na zminimalizowanie ryzyka naruszenia praw lub wolności osób fizycznych:

„Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku pseudonimizację i szyfrowanie danych osobowych".

Szyfrowanie to stary pomysł…

Termin „szyfrowanie" pochodzi od greckiego słowa: „kryptos", co oznacza ukryty, tajny. Jest to więc forma kryptografii polegająca na przekształceniu danych lub informacji w taki sposób, aby stały się nieczytelne dla nieupoważnionych osób. Zastosowanie szyfrowania można prześledzić już w starożytnym Egipcie, greckiej i rzymskiej kulturze wojskowej, przez wojny światowe i stworzenie pierwszego komputera, aż do jego współczesnego zastosowania w erze cyfrowej. Pierwszy odnotowany przypadek użycia szyfrowania pochodzi ze starożytnego Egiptu, kiedy to w pismach używano hieroglifów, które miały przysłonić pierwotne znaczenie tekstu. Na uwagę zasługuje również spartański wynalazek „scytale", który umożliwiał szyfrowanie wiadomości. Na drewnianą laskę nawijano skórzany cienki pasek, na którym następnie umieszczano konkretną wiadomość.
Po odwinięciu paska z cylindra tekst stawał się nieczytelny. Wyłącznie osoba, który była posiadaczem laski o identycznej grubości, po zawinięciu na nią otrzymanego paska z zaszyfrowaną wiadomością, mogła odczytać tekst. Innym przykładem szyfrowania jest tzw. „Szyfr Cezara", który był często używany przez Juliusza Cezara i wykorzystywał metodę podstawieniową, w której każda litera tekstu zastępowana jest inną, np. a->d, b->e, c->f…itd. Metoda podstawieniowa, jednak o znacznie wyższym stopniu zaawansowania, była wykorzystana w maszynie szyfrującej „Enigma", używanej przez niemieckie dowództwo wojskowe do szyfrowania strategicznych wiadomości przed i w czasie II wojny światowej. W 1932 roku Marian Rejewski, Jerzy Różycki i Henryk Zygalski wynaleźli system deszyfrujący, łamiąc tym samym kod Enigmy.

5 NOWE TECHNOLOGIE

… ale obecnie jest szczególnie potrzebne

Dynamiczny rozwój nowych technologii i rosnąca popularność inteligentnych urządzeń w naszym codziennym życiu, wymusiły wzrost zapotrzebowania na skuteczniejsze rozwiązania kryptograficzne. Ponadto z roku na rok rośnie liczba cyberataków i naruszeń bezpieczeństwa prowadzących do przypadkowego lub niezgodnego z prawem ujawnienia lub nieuprawnionego dostępu do danych osobowych.

W 2022 roku Urząd Ochrony Danych Osobowych zdecydował o nałożeniu administracyjnej kary pieniężnej w wysokości prawie 1,6 mln zł na P4 Sp. z o.o. z siedzibą w Warszawie, następcę prawnego Virgin Mobile Polska Sp. z o.o.

„Naruszenie przepisów RODO polegało na niewdrożeniu (…) odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych za pomocą systemów informatycznych. Systemy te służyły do rejestracji danych osobowych abonentów usług przedpłaconych, a brak zastosowanych w nich odpowiednich środków technicznych i organizacyjnych doprowadził do uzyskania przez osobę nieuprawnioną dostępu do tych danych, co stanowiło również naruszenie zasady integralności i poufności”.

Zdaniem organu nadzorczego przyjęte przez spółkę środki mogłyby być skuteczne, gdyby w ramach wdrożonych procedur zawierały również uregulowania dotyczące systematycznego testowania, mierzenia i oceniania skuteczności przyjętych środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Brak tego typu uregulowań i polityk szyfrowania znacznie osłabia bezpieczeństwo danych i informacji. W tym miejscu warto wspomnieć, że odpowiednie podejście do zarządzania bezpieczeństwem informacji w organizacji może zapewnić norma ISO 27001 standaryzująca systemy zarządzania bezpieczeństwem informacji (SZBI). W załączniku A normy ISO/IEC 27001 jest mowa o szyfrowaniu i zarządzaniu kluczami poufnych informacji. Obecnie istnieją dwa rodzaje algorytmów szyfrowania: symetryczny i asymetryczny. Główna różnica polega na tym, że szyfrowanie symetryczne używa tego samego klucza do szyfrowania i deszyfrowania danych, podczas gdy szyfrowanie asymetryczne wykorzystuje parę kluczy – klucz publiczny do szyfrowania danych i klucz prywatny do odszyfrowywania informacji, przy czym należy pamiętać, aby klucz prywatny był chroniony przed przechwyceniem przez osoby niepowołane. Przykładem szyfrowania symetrycznego może być wspomniany wyżej „Szyfr Cezara”. Współcześnie istnieją jednak bardziej złożone metody tego rodzaju szyfrowania. Za jedną z bezpieczniejszych uważa się standard Advanced Encryption Standard (AES) i jest on stosowany na całym świecie. Z kolei najpopularniejszym algorytmem szyfrowania asymetrycznego jest Rivesta-Shamira-Adlemana (RSA), które znajduje obecnie zastosowanie np. w szyfrowaniu korespondencji elektronicznej, czy protokołach kryptograficznych typu SSL/TLS.

5 NOWE TECHNOLOGIE

Kryptografia postkwantowa – czy stanie się elementem codzienności

Współczesne szyfry kryptograficzne są tworzone w taki sposób, aby ich deszyfracja trwała bardzo długo, dlatego w ostatnich latach poczyniono wiele inwestycji i innowacji w dziedzinie kryptografii. I tutaj pojawiają się komputery kwantowe, które mają potencjał złamania wielu obecnie stosowanych algorytmów kryptograficznych, w tym np. RSA o kluczu długości 2048 bitów, dlatego eksperci ds. cyberbezpieczeństwa wzywają do przyjęcia kryptografii postkwantowej, czyli algorytmów odpornych na włamanie za pomocą komputera kwantowego.
Nowe technologie szyfrowania będą miały kluczowe znaczenie dla zapewnienia bezpiecznego rozwoju ekosystemów cyfrowych, dlatego musimy być przygotowani na to, że w niedalekiej przyszłości konieczne będzie przyjęcie nowych, lepszych technologii szyfrowania, gdy tylko staną się one dostępne. Zanim to jednak nastąpi firmy powinny stosować aktualnie dostępne metody i techniki kryptograficzne w celu zapewnienia bezpieczeństwa i ochrony danych, zgodnie z motywem 83 RODO.

„W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko (…)”
Motyw 83 RODO

6 SPRAWY MIĘDZYNARODOWE

TSUE: ROZSTRZYGNIĘTO KWESTIĘ ŁĄCZENIA FUNKCJI IOD Z INNYMI ZADANIAMI W DANEJ ORGANIZACJI

Trybunał Sprawiedliwości Unii Europejskiej (TSUE) orzekł 9 lutego 2023 r., że IOD może mieć inne obowiązki w ramach swojej roli, jeśli nie występuje konflikt interesów. TSUE pozwala również sądom krajowym na określenie, co jest sytuacją konfliktu interesów, biorąc pod uwagę wszystkie istotne okoliczności, np. strukturę organizacyjną.

Artykuł 38 ust. 3 RODO zakazuje odwoływania inspektora ochrony danych, a art. 38 ust. 6 stanowi, że inspektor może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający muszą zapewnić, aby wszelkie takie zadania i obowiązki nie powodowały konfliktu interesów.
W ocenie Trybunału, RODO nie ustanawia zasadniczej niezgodności między sprawowaniem funkcji IOD a sprawowaniem innych funkcji u administratora danych lub jego podmiotu przetwarzającego.

„TSUE stwierdził, że IOD powinien „być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny", ale „nie można mu powierzyć zadań lub obowiązków, które prowadziłyby do określania przez niego celów i sposobów przetwarzania danych osobowych u administratora lub jego podmiotu przetwarzającego".

Orzeczenie TSUE zostało wydane w sprawie dotyczącej orzeczenia wstępnego niemieckiego Federalnego Sądu Pracy dla x-Fab Dresden i jego byłego IOD, który został zwolniony w wyniku pełnienia również funkcji przewodniczącego rady zakładowej.
Wyrok TSUE z dnia 9 lutego 2023 r. w sprawie C-453/21.

6 SPRAWY MIĘDZYNARODOWE

FINLANDIA: NIE MOŻNA LEKCEWAŻYĆ WNIOSKODAWCÓW, KTÓRZY KORZYSTAJĄ Z PRAW DO OCHRONY DANYCH

Fiński organ nadzorczy nałożył administracyjną karę pieniężną – 750 tys. euro – na przedsiębiorstwo windykacyjne za brak odpowiedzi na wnioski o wykonanie praw osób, których dane dotyczą. Firmie udzielono też upomnienia.

Fiński organ nadzorczy rozpoczął postępowanie w sprawie przedsiębiorstwa zajmującego się działalnością windykacyjną Alektum Oy po otrzymaniu trzech skarg od osób prywatnych. Dwie ze skarg dotyczyły tego, że administrator nie odpowiedział na wnioski o dostęp do danych osób, których dane dotyczą. Jeden ze skarżących otrzymał odpowiedź od administratora, ale nadal nie uzyskał żądanej kopii swoich danych osobowych.

Postępowanie prowadzone przez organ nadzorczy wykazało, że administrator regularnie nie udzielał odpowiedzi na wnioski dotyczące praw do ochrony danych przysługujących osobie, której dane dotyczą. Organ nadzorczy stwierdził, że administrator nie był wystarczająco zaznajomiony z wymogami prawa w zakresie ochrony danych osobowych, a jego działania wskazywały na obojętność wobec tych wymogów.

Administrator utrudniał i opóźniał również postępowanie, uchylając się od wezwań/zapytań organu nadzorczego.

Źródło: **decyzja organu nadzorczego**

LITWA: BEZ PODSTAWY PRAWNEJ NIE MOŻNA OGRANICZYĆ PRYWATNOŚCI PRACOWNIKA W MIEJSCU PRACY

Litewski organ nadzorczy przyjął decyzję w sprawie przetwarzania korespondencji osobistej pracownika.

Sprawa dotyczyła bezprawnego zwolnienia z pracy skarżącej przez dyrektora spółki będącej administratorem danych. Pracodawca wykorzystał jako podstawę zwolnienia osobistą korespondencję podwładnej na popularnym portalu społecznościowym z innym pracownikiem, zatrudnionym przez administratora.

Litewski organ nadzorczy uznał, że pracownik, pozostawiając na komputerze służbowym otwarte i niezabezpieczone hasłem konta społecznościowe, nie traci prawa do prywatności w miejscu pracy. Prywatność pracownika w miejscu pracy może być ograniczona przez odpowiednie środki monitorowania i kontroli stosowane przez pracodawcę w miejscu pracy, jednakże stosowanie takich środków musi być zgodne z wymogami RODO.

6 SPRAWY MIĘDZYNARODOWE

W świetle zasady rozliczalności (art. 5 ust. 2 RODO) administrator danych, nie uzasadnił podstawy prawnej zgodnego z prawem przetwarzania danych osobowych skarżącej (jej prywatnej korespondencji na portalu społecznościowym z innym pracownikiem administratora).
Organ nadzorczy uznał skargę za zasadną. Stwierdził, że administrator wykorzystał osobistą korespondencję skarżącej na portalu społecznościowym (sprawdzoną i wykorzystaną do wszczęcia postępowania dyscyplinarnego) bez podstawy prawnej z art. 6 ust. 1 RODO.

Źródło: **decyzja organu nadzorczego**

NAGRODY IM. STEFANO RODOTÀ 2023 ROZDANE

Czworo badaczy zajmujących się ochroną danych osobowych to tegoroczni laureaci Nagrody im. Stefano Rodoty, którą ustanowił Komitet Konwencji nr 108.

Nagroda honoruje pamięć Stefano Rodotà, włoskiego profesora prawa i polityka, który był orędownikiem promowania prawa do ochrony danych.

W 2023 roku spośród 31 otrzymanych zgłoszeń, jury złożone z członków Biura Komitetu Konwencji 108, przyznało:

- w kategorii *Prace dyplomowe*, Janis Ching Wong za pracę dyplomową zatytułowaną **„Co-creating data protection solutions through a Commons"**
- w kategorii *Artykuły*, Sebastiao Bernardo Bruco Geraldes de Barros Vale, Katerinie Demetzou i Gabrieli Zanfir-Fortuna, współautorom pracy zatytułowanej **„The Thin Red Line: Refocusing Data Protection Law on ADM, A Global Perspective with Lessons from Case-Law".**

Ponadto ponieważ regulamin nagrody na to pozwala, jury przyznało wyróżnienie specjalne Francesce Musiani i Ksenii Ermoshinie za pracę **„Concealing for Freedom: The Making of Encryption, Secure Messaging and Digital Liberties".**

8 PARTNERZY UODO

Bartłomiej Drozd
dyrektor Departamentu Rozwoju Produktów Konsumenckich Kaczmarski Group, ekspert ChronPESEL.pl.

POWSZECHNA OBAWA O PESEL

Ponad 60 proc. Polaków obawia się o swój PESEL, połowa zauważyła wzmożoną aktywność oszustów wyłudzających dane osobowe, a 15 proc. padło ofiarą ich utraty lub wycieku. I tylko 17 proc. ma absolutną pewność, że wie co robić, gdy ich dane trafią w niepowołane ręce. To najważniejsze wnioski z badania przeprowadzonego w styczniu 2023 roku na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów. To pokazuje z jak dużym zagrożeniem mamy do czynienia i jak bardzo ważne jest sprawne funkcjonowanie systemu chroniącego nasze dane osobowe.

Żyjemy w czasach, w których Internet odgrywa ważną rolę w życiu każdego. Ułatwia życie, ale też niesie zagrożenia. Wiele osób nie zdaje sobie jeszcze sprawy z tego, że dane wszystkich nas są w sieci. Urzędy, przychodnie, banki, sklepy internetowe i wiele innych firm i instytucji przechowuje je w swoich zasobach. Jedne są chronione dobrze, inne nie. Wśród nich znajduje się również nasz numer PESEL. W styczniu 2023 roku 15 proc. ankietowanych przez nas Polaków przyznało, że padło ofiarą wycieku lub kradzieży danych osobowych, a co 5. (21 proc.) nie potrafi jednoznacznie stwierdzić, czy tak nie było. Jeśli wspomniane 15 proc. odnieść do populacji dorosłych Polaków, oznaczałoby to, że swoje dane utraciło ponad 4,5 mln Polaków, a mówimy tylko o tych, którzy wiedzą, że do tego doszło.

Wszystkie nasze sprzęty podłączone są do Internetu: telefon, komputer czy też laptop. A to właśnie dzięki Internetowi hakerzy mogą włamać się na nasze urządzenia i wykraść ważne dla nas dane. Tego obawia się 60 proc. badanych. Na drugim miejscu (57 proc.) wśród wskazywanych zagrożeń dla bezpieczeństwa danych osobowych jest phishing, czyli podszywanie się pod firmy i instytucje. Oczywiście nie są to jedyne sposoby w jakie nasze dane mogą trafić w niepowołane ręce. 52 proc. ankietowanych nie ufa, że bazy danych, na których przechowywane są wszelakie informacje, są dobrze chronione. Najmniej (48 proc.) boi się fizycznej kradzieży dokumentów.

8 PARTNERZY UODO

I tylko w tym ostatnim przypadku możemy być pewni, że padliśmy ofiarą przestępstwa. Gdy mamy do czynienia z włamaniem do komputera czy do jakiejś bazy danych, często nie mamy nawet świadomości, że nasze dane osobowe trafiły w niepowołane ręce i mogą być wykorzystane na naszą szkodę. Hakerzy często nie zostawiają śladów, a dane osobowe, to tylko cyfrowy zapis, który można skopiować. Świadomość tego jest dość duża, bo zaledwie 16 proc. respondentów była absolutnie pewna, że ich dane nigdy nie trafiły w niepowołane ręce.

To nie znaczy, że jesteśmy w tej walce bezbronni. Ochronę powinny nam zapewnić odpowiednie regulacje prawne i urzędy, które stoją na straży ich przestrzegania. Nieocenioną rolę odgrywa tu Urząd Ochrony Danych Osobowych, z którym mamy zaszczyt od 2 lat współpracować w edukowaniu Polaków na temat tego, jak chronić swoje dane osobowe, na jakie niebezpieczeństwa uważać, jakich błędów nie popełniać. Ale to za mało. Pewnie nigdy nie uda się stworzyć tak szczelnego systemu, który ustrzeże nas przed niebezpieczeństwem. Gospodarka cyfrowa niesie też ze sobą pewne zagrożenia, którym przeciwdziałać można tylko aktywnie monitorując nieautoryzowane użycie naszych danych osobowych, w tym numeru PESEL. Musimy pamiętać o tym, że to przede wszystkim nasze dane i nasz kłopot, kiedy trafią w niepowołane ręce.

www.uodo.gov.pl