Nr 6/2022 (39)
Czerwiec 2022

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

4 LATA RODO Z PERSPEKTYWY UODO

KOMENTARZE EKSPERTÓW

JAN NOWAK

Prezes Urzędu Ochrony Danych Osobowych

Szanowni Państwo,
za nami 4 lata stosowania ogólnego rozporządzenia o ochronie danych - RODO. Warto podkreślić, że jest to akt, który bezpośrednio obowiązuje we wszystkich państwach członkowskich Unii Europejskiej, w sposób jednolity regulując prawa obywateli i obowiązki administratorów.

Ogólne rozporządzenie ma na celu ochronę praw wszystkich osób fizycznych, a jednocześnie zapewnia właściwy balans między prawami administratorów, w tym przedsiębiorców i organów publicznych, a prawami osób, których dane dotyczą.

W codziennej pracy Urzędu Ochrony Danych Osobowych kierujemy się tym, że prawo do ochrony danych osobowych jest prawem podstawowym każdego człowieka, w szczególności gwarantowanym przez Konstytucję RP. Dlatego tak ważne jest, aby Urząd był blisko obywateli, co staramy się robić na co dzień, także w kontekście zmian organizacyjnych, które wprowadziliśmy rok po naszych doświadczeniach w stosowaniu RODO. Jestem przekonany, że w dłuższej perspektywie przełoży się na lepszą ochronę danych osobowych w Polsce, bo już teraz widzimy, że liczba wpływających skarg do Urzędu z roku na rok rośnie. Podobnie jest ze zgłaszaniem naruszeń ochrony danych osobowych. W roku 2021 do UODO wpłynęło ponad 8300 skarg oraz prawie 13000 naruszeń.

25 maja jest dniem, w którym wyraźnie widzimy, że właściwe wdrożenie RODO nie było i nie jest zadaniem jednorazowym, lecz ciągłym procesem. Z czasem wszyscy zdobywają coraz większą wiedzę o wymogach przewidzianych przez RODO oraz lepiej potrafią chronić prawa i wolności osób, których dane dotyczą. Widzimy, że nasza wspólna wytężona praca miała i ma sens, lecz mamy też świadomość nowych wyzwań, przed którymi stoją wszystkie osoby zajmujące się ochroną danych osobowych.

Co przed nami? Nowe technologie towarzyszą nam każdego dnia już od dawna. Jednakże czas trwania pandemii COVID-19 i konieczność zastosowania rozwiązań, takich jak świadczenie pracy w trybie zdalnym, realizacja nauczania dzieci i młodzieży metodami na odległość czy wzrost korzystania z e-usług, spowodował znaczne przyspieszenie transformacji cyfrowej. Aby promować prorozwojowe technologie, Komisja Europejska przedstawiła wizję i kierunek transformacji cyfrowej w Europie do 2030 r., proponując kompas cyfrowej dekady w UE. W związku z tym czekamy na nowe unijne przepisy, które będą miały wpływ na ochronę danych osobowych i prywatności wszystkich obywateli. Wśród projektowanych regulacji należy wymienić: Akt o usługach cyfrowych, Akt o rynkach cyfrowych, czy też Akt o zarządzaniu danymi. Należy także wspomnieć o pracach nad Aktem o sztucznej inteligencji, Aktem o danych, czy projektem rozporządzenia w sprawie budowy europejskiej przestrzeni danych dotyczących zdrowia.

Sądzę, że w najbliższym czasie wyzwaniem na kolejne lata będzie zapewnienie harmonii i spójności przepisów RODO ze wszystkimi unijnymi aktami, które mają na celu uregulowanie technologii lub działalności związanej z przetwarzaniem danych osobowych. To istotne, aby cały system prawny pozwolił rozwijać się gospodarce opartej o dane z poszanowaniem praw i wolności obywateli.

MONIKA KRASIŃSKA
dyrektor Departamentu Orzecznictwa i Legislacji

Po 4 latach stosowania RODO można stwierdzić, że większość zakładanych celów tej regulacji została osiągnięta – wzrosła świadomość wagi i potrzeby ochrony danych osobowych, zwiększyła się samodzielność i odpowiedzialność administratorów, a obowiązujące w organizacjach rozwiązania i procedury w zakresie ochrony danych osobowych zostały dostosowane do RODO i są stosowane na co dzień. Wiązało się to z wykonaniem ogromnej pracy.

Doświadczenia UODO wskazują, że ci administratorzy, którzy przed czterema laty ze spokojem podeszli do wdrożenia RODO, z odpowiednim wyprzedzeniem i ze zrozumieniem odczytali regulacje zreformowanego systemu ochrony danych osobowych, nie mieli większych problemów ze spełnieniem nowych obowiązków. Byli jednak i tacy, którzy działali na ostatnią chwilę, bez znajomości i zrozumienia określonych w RODO zasad. Dodatkowo, w szumie medialnym związanym z RODO, pojawiło się wiele mitów czy półprawd, a na rynku uaktywniły się firmy próbujące zarobić na niewiedzy w tym zakresie.

Uważam, że aktywne, a jednocześnie zdroworządkowe działanie UODO pozwoliło na uspokojenie nastrojów i wyjaśnienie wszystkich wątpliwości. Służyły temu m.in.: wydawane przez Urząd poradniki, zamieszczane na stronie internetowej materiały, cykliczna publikacja „Newslettera UODO dla IOD", odpowiedzi udzielane zarówno na pytania od inspektorów ochrony danych oraz administratorów, jak i od osób, których dane dotyczą, czy też warsztaty i szkolenia organizowane dla IOD i administratorów stosujących nowe przepisy o ochronie danych osobowych.

Oczywiście te wytyczne, wskazówki czy zalecenia były jedynie pewnymi podpowiedziami. Ostatecznym bowiem architektem procesu przetwarzania danych osobowych, prowadzonego z poszanowaniem obowiązujących przepisów sektorowych, jest sam administrator.

Ważnym zadaniem organu nadzorczego były i są działania na rzecz tworzenia przewidzianych w RODO kodeksów postępowania oraz zachęcanie kolejnych branż do podejmowania takich inicjatyw. Szczególnie istotne były prace nad zamknięciem systemu przyjmowania kodeksów postępowania, tak by umożliwić ich zatwierdzenie, tj. prace nad określeniem wymogów akredytacji podmiotów monitorujących. Doprowadziły one do przedstawienia „Wymogów akredytacji podmiotów monitorujących przestrzeganie postanowień kodeksów postępowania" i ich pozytywnego zaopiniowania przez Europejską Radę Ochrony Danych, a wcześniej skonsultowania z zainteresowanymi krajowymi środowiskami. Warto w tym miejscu podkreślić, że eksperci

UODO aktywnie uczestniczyli w pracach EROD nad przyjętymi Wytycznymi 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679. Zatwierdzenie kodeksów postępowania przez Prezesa UODO i rozpoczęcie ich stosowania będzie kolejną inicjatywą wspierającą administratorów i podmioty przetwarzające w odpowiedniej organizacji procesów przetwarzania danych osobowych w danej branży, podnosząc ich poziom. Ten pozytywny aspekt stosowania kodeksów będzie też odczuwalny przez osoby, których dane są przetwarzane, gdyż będą one mogły liczyć na podwyższony standard ochrony ich danych osobowych przez daną branżę.

Te konsekwentne działania organu nadzorczego, zapewniające wielu różnym środowiskom wsparcie eksperckie, przynoszą zamierzone rezultaty.

Sukcesy możemy odnotować też na polu legislacyjnym. Na skutek uwag wniesionych w toku prac legislacyjnych udało się wprowadzić wiele zmian wzmacniających ochronę naszych danych osobowych. Odnotować jednak trzeba, że niektóre organy publiczne – wbrew obowiązkowi – pomijały proces uzgodnień i opiniowania, i nie przekazywały do oceny organu nadzorczego istotnych projektów aktów normatywnych dotyczących przetwarzania danych osobowych lub zawierających regulacje w tym zakresie. W części przypadków projekty te były konsultowane dopiero przez Rządowe Centrum Legislacji oraz Kancelarię Sejmu, które przekazywały część tych projektów do Prezesa UODO, na właściwych dla tych podmiotów etapach prac legislacyjnych.

W zakresie ochrony danych osobowych jest też wiele wyzwań, z którymi w najbliższym czasie trzeba będzie się zmierzyć. Jednym z nich jest potrzeba dokończenia przeglądu krajowych przepisów prawa pod kątem zapewnienia ich zgodności z RODO. Analiza taka, przeprowadzona w 2018 roku w związku z rozpoczęciem stosowania RODO i zakończona wprowadzeniem w porządku prawnym szeregu zmian ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, mimo że obejmowała wiele aktów prawnych, nie była pełna i wymaga kontynuacji. Nie podjęto np. wysiłku dostosowania do RODO prawodawstwa w zakresie tak istotnej kwestii, jak dostęp do informacji publicznej. Kolejnym istotnym zagadnieniem jest niewłaściwa implementacja tzw. dyrektywy policyjnej, która w praktyce powoduje wątpliwości interpretacyjne.

W dalszym ciągu przedmiotem szczególnego zainteresowania organu nadzorczego będą też takie zagadnienia, jak: przebudowywanie i tworzenie nowych rejestrów publicznych, wywiązywanie się przez projektodawców z obowiązku przeprowadzenia oceny skutków dla ochrony danych, projektowanie nowych rozwiązań cyfrowych ingerujących w prywatność osób, ochrona krajowego numeru identyfikacyjnego – PESEL, monitoring wizyjny czy przetwarzanie szczególnych kategorii danych.

Ochrona danych osobowych staje się integralną częścią modelu rozwoju usług publicznych i usług komercyjnych, gdyż coraz więcej naszych życiowych i zawodowych aktywności realizowanych jest w świecie Internetu. Dane osobowe stały się jednym z najcenniejszych zasobów i wobec coraz szybszego rozwoju technologicznego przetwarzający dane osobowe muszą podążać za dynamiką zmian i nie mogą stać w miejscu. Wdrażanie RODO to niekończący się proces, nieustanne dostosowywanie przyjętych rozwiązań do stale zmieniających się warunków tak, by w danym momencie zapewnić zgodność swojego działania z RODO. Inaczej rzecz ujmując, ochrona danych osobowych to nie tylko przepisy, które trzeba stosować, ale cały system, w którym każdy pełni ważną rolę i który na stałe jest wpisany w zarządzanie organizacją. Proces planowy, podlegający co jakiś czas audytowi, a nie jedynie reakcja na zmiany prawa czy zdarzające się incydenty.

JACEK MŁOTKIEWICZ
dyrektor Departamentu Kontroli i Naruszeń

Właśnie upływa 4 rok stosowania RODO, które wprowadziło istotne zmiany w podejściu do ochrony danych osobowych poprzez wprowadzenie dla administratorów nowych obowiązków w tym zakresie, czy też poważną modyfikację już istniejących. Wymusiło to na administratorach konieczność całkowicie innego spojrzenia na funkcjonujący w ich organizacji system ochrony danych w celu oczywiście dostosowania go do nowych wymogów. W tych początkach stosowania RODO, podsycanych jeszcze dodatkowo strachem przed wielomilionowymi karami za naruszenie jego przepisów, bardzo ważna była rola Urzędu Ochrony Danych Osobowych jako tego, który ma wskazać właściwą ścieżkę postępowania i pomóc administratorom w możliwie najmniej bolesnym dostosowaniu się do nowych warunków przetwarzania danych osobowych wykreowanych przez RODO. W pierwszym okresie stosowania RODO na tym koncentrowały się działania organu nadzorczego, budując tym samym pewną określoną praktykę stosowania tych przepisów. Te działania przejawiały się na wielu płaszczyznach. Przede wszystkim przygotowane zostały określone formularze, które miały pomóc administratorom w prawidłowej realizacji ich obowiązków wynikających z RODO, w tym obowiązków notyfikacyjnych. Najlepszym przykładem jest formularz dotyczący zgłaszania naruszeń ochrony danych osobowych. Formularz ten nie tylko zapewnia administratorowi danych przekazanie organowi nadzorczemu wszystkich wymaganych przez RODO informacji, ale także tych, które pomagają nie tylko organowi nadzorczemu na ocenę zaistniałego naruszenia, ale i samemu administratorowi danych na analizę przyczyn jego wystąpienia i wybór najlepszych środków naprawczych. Kolejnym przykładem działań organu nadzorczego, które ukształtowało praktykę postępowania administratorów była propozycja dotycząca sposobu prowadzenia rejestru czynności przetwarzania danych osobowych, gdzie jako przykład podano czynność związaną z przetwarzaniem danych osobowych pracowników. Oprócz tego na stronie internetowej UODO zamieszczonych zostało wiele porad, wskazówek, czy wytycznych dotyczących praktycznych aspektów stosowania RODO, których celem było podpowiedzenie administratorom danych jak postępować, by w sposób prawidłowy wywiązać się z nowych obowiązków nałożonych na nich przez RODO.

Wydaje się, że działania informacyjno-edukacyjne przyniosły zamierzony skutek. Z roku na rok do UODO jest zgłaszanych coraz więcej naruszeń ochrony danych osobowych. W roku 2019 roku Urząd dokonał analizy 6039 zgłoszeń naruszeń m.in. pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Wówczas najwięcej naruszeń zgłaszały podmioty prywatne, w szczególności prowadzące działalność w sektorach telekomunikacyjnym, ubezpieczeniowym oraz finansowym. W przypadku podmiotów publicznych najczęściej zgłaszano naruszenia w jednostkach samorządu terytorialnego, placówkach oświaty oraz służby zdrowia. Rok 2020 to z kolei analiza nieco ponad 7500 zgłoszeń naruszeń również przede wszystkim pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Trzeba podkreślić, że w tym roku zgłaszano wiele naruszeń związanych z zagrożeniem epidemicznym, które wymogło na administratorach niezwłoczne podejmowanie dodatkowych środków w celu ochrony zdrowia osób, których dane dotyczą. To z kolei wiązało się z wystąpieniem incydentów bezpieczeństwa w sferach, które nie były wcześniej poddawane szczegółowej analizie pod kątem wystąpienia możliwych zagrożeń

i podatności na zagrożenia. Zauważalne jest, że w okresie pandemii zwiększyła się liczba naruszeń ochrony danych osobowych związanych z ransomware. Jest to powiązane m.in. z koniecznością przejścia podmiotów na tryb pracy zdalnej, podczas której w sposób nieodpowiedni zabezpieczone zostają połączenia pomiędzy komputerami użytkowników a serwerami, na których znajdują się aktywa/zasoby danego podmiotu. W czasie pandemii koronawirusa dochodziło również do naruszeń ochrony danych osobowych polegających na ujawnieniu danych osób objętych kwarantanną medyczną, które miały kontakt z osobami z pozytywnym wynikiem testu na obecność SARS-CoV-2.

W 2021 roku do Urzędu Ochrony Danych Osobowych wpłynęło przawie 13 tys. zgłoszeń naruszeń.

Ten sukcesywny wzrost liczby zgłoszeń naruszeń ochrony danych osobowych do UODO wynika z jednej strony z coraz większej świadomości administratorów, co do ich obowiązków wynikających RODO, z drugiej – z obawy przed konsekwencjami, w tym przed nałożeniem administracyjnej kary pieniężnej.

Nie można zapomnieć także o działaniach kontrolnych organu nadzorczego, które powodują kształtowanie się określonej praktyki, szczególnie wówczas gdy takim kontrolom poddawany jest określony sektor. To jest bowiem jedno z najważniejszych narzędzi znajdujących się w dyspozycji organu nadzorczego. Pozwala ono szybko i na miejscu (w siedzibie podmiotu kontrolowanego) dokonać ustaleń w zakresie przestrzegania przepisów RODO przy przetwarzaniu danych osobowych i wskazać ewentualne nieprawidłowości w tym zakresie.

PAULINA DAWIDCZYK

dyrektor Departamentu Skarg

W 2018 roku, obserwując dyskusję na temat wdrożenia ogólnego rozporządzenia o ochronie danych osobowych (RODO), miałam wrażenie, że przepisy dotyczące ochrony danych osobowych dopiero zaczynają funkcjonować w naszym kraju, a przecież one obowiązywały od ponad 20 lat. RODO jedynie wprowadziło dodatkowe obowiązki na administratorów, ale przepisy dotyczące ochrony danych osobowych są z nami od dawna. Po wejściu w życie nowych unijnych przepisów baczniej zaczęto zwracać uwagę na kwestię ochrony danych osobowych. RODO na pewno uświadomiło wielu osobom i administratorom, że warto lepiej dbać o dane osobowe i o prywatność.

Po 4 latach stosowania RODO zauważam, że Polacy mają świadomość istnienia rozporządzenia. Znają, chociażby hasłowo, przysługujące im poszczególne prawa, co sytuuje nas w czołówce państw europejskich. Świadomość to jednak jedno, jakość wiedzy – drugie, a budowanie odpowiednich postaw społeczeństwa to trzecie.

W Polsce sama wiedza na temat ochrony danych osobowych czy przysługujących nam praw jest na wysokim poziomie. Wzrost świadomości społeczeństwa jest widoczny, co potwierdza liczba składanych do Urzędu Ochrony Danych Osobowych skarg na nieprawidłowe przetwarzanie danych. Liczba skarg gwałtownie wzrosła od 2018 roku. W 2017 roku było ich nieco ponad 2,9 tys., a w całym 2018 roku było ich już ponad 5,5 tys. W 2019 roku do organu nadzorczego wpłynęły

9304 skargi, tj. o 3739 więcej w stosunku do roku 2018. W 2019 roku zakres tematyczny skarg był bardzo szeroki. Dotyczył on wszelkich aspektów przetwarzania danych osobowych, a także odnosił się do szerokiego kręgu podmiotów - zarówno z sektora prywatnego jak i publicznego. Do najczęściej składanych skarg zaliczano pozyskiwanie danych osobowych bez podstawy prawnej, wykorzystanie urządzeń rejestrujących zarówno przez osoby fizyczne, jak i monitoringu wizyjnego stosowanego przez różnego rodzaju podmioty czy przekazywanie danych firmom windykacyjnym i do BIK bez podstawy prawnej bądź w sposób nieprzejrzysty dla osób, których te dane dotyczą. Skargi dotyczyły również kwestii pracowniczych jak dopuszczalny zakres danych oraz przesłanek legalizujących wykorzystywanie danych przez pracodawców, w tym przekazywanie danych osobowych pracowników podmiotom zewnętrznym.

Biorąc pod uwagę, że liczba skarg wpływających do UODO w przedmiocie nieprawidłowości w procesie przetwarzania danych osobowych gwałtownie wzrosła po 25 maja 2018 r., kluczowa była sprawna obsługa obywateli w tym zakresie. Zmiany w strukturze organizacyjnej Urzędu były konsekwencją doświadczeń wynikających z funkcjonowania w latach 2018–2019 zespołów tematycznych.

Rok 2020 był pierwszym pełnym rokiem funkcjonowania Departamentu Skarg w strukturach Urzędu. Pomimo światowej pandemii koronawirusa w roku 2020 do UODO wpłynęły w sumie 6442 skargi. W 2020 r. przedmiotem wpływających do UODO skarg było przetwarzanie danych w celach marketingowych. Najczęściej skarżący wskazywali na otrzymywanie połączeń telefonicznych od nieznanych im wcześniej podmiotów i notoryczne otrzymywanie niechcianych wiadomości e-mail o charakterze marketingowym, gdy nie posiadali wiedzy o źródle pozyskania ich danych przez te podmioty.

Z kolei w 2021 rok odnotowano ponad 8300 skarg, tj. o ok. 1800 skarg więcej w stosunku do roku poprzedniego. W tym czasie skarżący podnosili w skargach przetwarzanie danych osobowych przez administratora w celu innym niż cel, do którego dane te zostały pozyskane, niedopełnienia obowiązku informacyjnego wobec osoby, której dane dotyczą, oraz niedostarczenia osobie, której dane dotyczą, kopii danych osobowych podlegających przetwarzaniu przez administratora. Do UODO wpływały także skargi dotyczące przetwarzania danych osobowych przez spółdzielnie oraz wspólnoty mieszkaniowe czy przetwarzania wizerunku utrwalonego za pomocą monitoringu wizyjnego. Ponadto do UODO składano skargi dotyczące przetwarzania danych w związku z pandemią COVID-19 oraz plików cookies na stronach internetowych.

Przytoczone dane statystyczne potwierdzają, że przepisy prawa, takie jak zawarte w RODO, dają nam konkretne narzędzia w postaci praw gwarantowanych, dzięki którym możemy skuteczniej przeciwdziałać wielu zagrożeniom. Co prawda zakres przedmiotowy tych skarg jest od kilku lat bardzo podobny, to należy wskazać, że przed nami pojawiają się także nowe wyzwania, na które z pewnością ma wpływ powszechne przyspieszenie transformacji

URSZULA GÓRAL

dyrektor Departamentu Współpracy Międzynarodowej i Edukacji

Minione 4 lata stosowania RODO wzbogaciły nas w wiele cennych doświadczeń. Nieustanna obserwacja warunków społeczno-gospodarczych, a także analiza otoczenia prawno-instytucjonalnego, w jakim działają administratorzy, postawiła nas przed wieloma wyzwaniami, które dotyczą m.in. edukacji. Z tego względu UODO realizował różnorodne działania edukacyjne. Były to głównie konferencje, webinaria, szkolenia, publikacje poradnikowe oraz kampanie edukacyjne organizowane wspólnie z innymi podmiotami, które były skierowane przede wszystkim do administratorów oraz inspektorów ochrony danych, ale też wszystkich zainteresowanych ochroną danych osobowych. Obchodzony co roku Dzień Ochrony Danych Osobowych, przypadający na 28 stycznia, stanowi również okazję do podejmowania wielu inicjatyw. Wspólnym celem tych działań było i nadal pozostanie upowszechnianie w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych i rozumieniem tych zjawisk. Wspieramy także edukację w szkołach wyższych, w tym zwłaszcza w ramach szerokiej oferty studiów podyplomowych.

Jako organ nadzorczy szczególną uwagę poświęcamy działaniom skierowanym do dzieci. Jesteśmy bardzo dumni z tego, jak wiele informacji o ochronie danych osobowych czerpią nauczyciele i uczniowie, uczestnicząc w ogólnopolskim programie edukacyjnym „Twoje dane – Twoja sprawa". Program stanowi doskonałe źródło wiedzy i dobrych praktyk w zakresie ochrony danych osobowych w szkołach oraz realizacji obowiązków wynikających z RODO w sektorze oświaty.

Rezultatem podejmowanych działań edukacyjnych jest kształtowanie prawidłowych postaw i nawyków wśród dzieci i młodzieży, popularyzacja wiedzy na temat skutecznej ochrony danych osobowych wśród uczniów i nauczycieli, wzrost zainteresowania tematem oraz współpraca społeczności szkolnej i środowiska lokalnego na rzecz upowszechniania wiedzy o ochronie danych osobowych.

Każdego roku w programie bierze udział ponad 45 tys. uczniów i ponad 4000 nauczycieli, którzy podejmują różne działania edukacyjne na rzecz upowszechniania wśród uczniów wiedzy o ochronie danych osobowych i prawa do prywatności. Co roku odbywa się ponad 1000 inicjatyw edukacyjnych skierowanych do uczniów, nauczycieli, rodziców, seniorów i środowiska lokalnego.

Zaangażowanie i otwartość uczestników programu, chęć podnoszenia wiedzy o ochronie danych osobowych czy bogactwo pomysłów na prowadzenie zajęć edukacyjnych na temat prywatności wśród dzieci i młodzieży, potwierdzają, że zapotrzebowanie na tak szczególne informacje nie wynika wyłącznie z pojawienia się RODO i konieczności jego stosowania również w szkołach. Ma to także związek ze wzrostem świadomości społeczeństwa, również wśród młodego pokolenia, które dostrzega, że RODO dotyczy spraw im bliskich i ważnych, z jakimi mają lub w przyszłości będę mieć do czynienia na co dzień.

Co istotne, UODO uczestniczy w pracach europejskich i międzynarodowych organizacji działających na rzecz ochrony danych osobowych. Co więcej, w ramach współpracy na forum Europejskiej Rady Ochrony Danych, której UODO jest członkiem, Urząd aktywnie uczestniczy w opracowywaniu opinii, wytycznych,

zaleceń i najlepszych praktyk w celu promowania wspólnego zrozumienia RODO i dyrektywy 2016/680, a także bierze udział w doradzaniu Komisji Europejskiej w kwestiach związanych z ochroną danych osobowych w UE. Przedstawiciele Urzędu angażują się również, w ramach EROD, w działania promujące współpracę pomiędzy organami nadzorczymi z UE oraz EOG. W ciągu ostatnich 4 lat organy nadzorcze zainwestowały wiele zasobów w interpretację i spójne stosowanie RODO, zatwierdzając i przyjmując aż 57 wytycznych i 6 zaleceń. Od rozpoczęcia stosowania RODO, UODO współpracuje z innymi organami także wymieniając się, za pośrednictwem systemu wymiany informacji na rynku wewnętrznym – IMI, w sposób bezpieczny i ustandaryzowany, informacjami niezbędnymi dla realizacji mechanizmów współpracy i spójności, o których mowa w rozdziale VII RODO, i w tym zakresie prowadzi postępowania transgraniczne. UODO jest także członkiem Komitetu Konsultacyjnego do spraw Konwencji o Ochronie Osób w związku z Automatycznym Przetwarzaniem Danych Osobowych (Komitet T-PD) Rady Europy. W 2019 roku Polska ratyfikowała Protokół zmieniający Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Protokół wprowadził tzw. Konwencję 108+, której celem jest ochrona prywatności obywateli w nowej erze cyfrowej.

Po 4 latach stosowania RODO, patrząc na kolejne wyzwania, jakie stoją przed UODO i innymi organami nadzorczymi, należy podkreślić, że w najbliższych latach fundamentalne znaczenie będzie miało osadzenie RODO i organów nadzorczych w regulacjach opracowywanych na potrzeby rynku cyfrowego. Co więcej, kluczowe będzie zapewnienie jasnego podziału kompetencji między organami regulacyjnymi, a także skutecznej współpracy pomiędzy organami.

PRZECHOWYWANIE AKTU URODZENIA DZIECKA W AKTACH OSOBOWYCH PRACOWNIKA

Przepisy prawa pracy są podstawą uprawniającą pracodawcę do przechowywania aktu urodzenia dziecka w aktach osobowych pracownika chcącego skorzystać z urlopu rodzicielskiego.

Urlop rodzicielski to jedno z określonych przepisami Kodeksu pracy uprawnień przysługujących ojcu i matce dziecka, a także rodzicom adopcyjnym.

Zgodnie z § 2 ust. 2 oraz § 4 ust. 2 rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 8 grudnia 2015 r. w sprawie wniosków dotyczących uprawnień pracowników związanych z rodzicielstwem oraz dokumentów dołączanych do takich wniosków, do wniosku, o którym mowa w art. 179^1 § 1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy, tj. do wniosku o udzielenie pracownicy lub pracownikowi, bezpośrednio po urlopie macierzyńskim, urlopu rodzicielskiego w pełnym wymiarze, dołącza się skrócony odpis aktu urodzenia dziecka (dzieci) lub zagraniczny akt urodzenia dziecka (dzieci) albo kopie tych dokumentów, albo kopię zaświadczenia lekarskiego wystawionego na zwykłym druku, określającego przewidywaną datę porodu. Stosownie zaś do § 4 ust. 4 powołanego rozporządzenia, przepisy ust. 1–3 stosuje się odpowiednio do wniosku o udzielenie urlopu rodzicielskiego złożonego przez

pracownika, który przyjął dziecko na wychowanie i wystąpił do sądu opiekuńczego z wnioskiem o wszczęcie postępowania w sprawie przysposobienia dziecka lub przyjął dziecko na wychowanie jako rodzina zastępcza.

Z kolei zakres, sposób i warunki prowadzenia oraz przechowywania dokumentacji pracowniczej określa rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej. Stanowi ono, że akta osobowe pracownika składają się z czterech części i wskazuje, jaki rodzaj oświadczeń i dokumentów znajduje się w każdej z nich.

Zgodnie z § 3 pkt 2 lit. m tego rozporządzenia, w części B akt osobowych pracownika gromadzone są dokumenty związane z ubieganiem się i korzystaniem przez pracownika z urlopu macierzyńskiego, urlopu na warunkach urlopu macierzyńskiego, urlopu rodzicielskiego, urlopu ojcowskiego lub urlopu wychowawczego.

Zatem to powołane wyżej przepisy uprawniają pracodawcę do przechowywania w części B akt osobowych pracownika zarówno wniosku o urlop rodzicielski, jak i dołączanego do niego skróconego odpisu aktu urodzenia dziecka (dzieci) lub zagranicznego aktu urodzenia dziecka (dzieci) albo kopii tych dokumentów.

Jednocześnie warto przypomnieć o konieczności przestrzegania odpowiednich okresów przechowywania danych, w określeniu których pomocny może być zamieszczony na stronie internetowej UODO materiał „Czy z dokumentacji pracowniczej należy usuwać dane nadmiarowe?”.

WYMIANA INFORMACJI MIĘDZY SZKOŁĄ A PLACÓWKĄ WSPARCIA DZIENNEGO

Wymiana między szkołą a placówką wsparcia dziennego takich informacji o dziecku, jak m.in. wyniki w nauce, frekwencja, potrzeby rozwojowe i edukacyjne, zachowania oraz funkcjonowanie społeczne, jest możliwa bez zgody jego rodziców lub opiekunów. Podstawą uprawniającą do takiego działania są przepisy ustawy o wspieraniu rodziny i systemie pieczy zastępczej.

Placówki wsparcia dziennego to jedne z podmiotów, które wspierają rodziny przeżywające trudności w wypełnianiu funkcji opiekuńczo wychowawczych. Są one prowadzone na podstawie ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej przez gminę lub powiat, podmiot, któremu gmina lub powiat zleciły realizację tego zadania na podstawie art. 190, albo przez podmiot, który uzyskał zezwolenie wójta bądź starosty.

Placówki wsparcia dziennego, realizując zadania wynikające z powołanej ustawy, mają, zgodnie z art. 23 ust. 1, współpracować z rodzicami lub opiekunami dziecka, a także z placówkami oświatowymi i podmiotami leczniczymi. W związku z tym konieczne bywa wzajemne przekazywanie informacji dotyczących m.in.: wyników w nauce, zachowania czy potrzeb rozwojowych i edukacyjnych oraz funkcjonowania społecznego dziecka.

Ponadto przepisy powołanej ustawy stanowią (art. 8 ust. 3), że wspieranie rodziny jest prowadzone za jej zgodą i aktywnym udziałem. W związku z tym powstają wątpliwości, czy na wymianę informacji między szkołą a placówką wsparcia dziennego trzeba pozyskiwać zgodę rodziców lub opiekunów prawnych.

W opinii UODO obowiązek współpracy placówki wsparcia dziennego z osobami i podmiotami wskazanymi w art. 23 ustawy o wspieraniu rodziny i systemie pieczy zastępczej opiera się na zgodzie rodziny i jej aktywnym udziale, o czym stanowi art. 8 ust. 3 ustawy. U podstaw owej współpracy leży wartość, jaką jest dobro dziecka w rozumieniu art. 72 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., zaś współdziałanie określonych podmiotów podejmowane w jej ramach ma służyć poprawie realizacji funkcji opiekuńczo-wychowawczej przez rodzinę lub opiekunów dziecka, a w konsekwencji poprawie sytuacji samego dziecka. Odczytując przepisy ustawy o wspieraniu rodziny i systemie pieczy zastępczej przez pryzmat standardów wykładni funkcjonalnej i systemowej uznać należy, że zgoda rodziców lub opiekunów dziecka na określone działania podejmowane przez określone podmioty jest wymagana jedynie w szczególnych (nadzwyczajnych) sytuacjach, w których dochodzi do istotnej ingerencji w sferę władzy rodzicielskiej w rozumieniu ustawy z dnia 25 lutego 1964 r. – Kodeks rodzinny i opiekuńczy. Wydaje się, że w kontekście omawianej ustawy brak konieczności pozyskiwania zgody rodziców lub opiekunów prawnych na działania nieingerujące w sferę władzy rodzicielskiej jest uzasadniony zwłaszcza wówczas, gdy rodzina przyjmuje pozycję bierną w procesie współpracy z placówką wsparcia dziennego.

Natomiast podstawę prawną wymiany informacji dotyczących m.in. wyników w nauce, frekwencji, potrzeb rozwojowych i edukacyjnych, możliwości psychofizycznych, zachowania w szkole lub placówce wsparcia dziennego oraz funkcjonowania społecznego dziecka, dokonywanej między placówką wsparcia dziennego a placówką oświatową, stanowi art. 18 ustawy o wspieraniu rodziny i systemie pieczy zastępczej w zw. z art. 23 ust. 1 tej ustawy. Przepisy te i wynikające z nich obowiązki powinny być interpretowane ze szczególnym uwzględnieniem zasad ogólnych zawartych w art. 5 RODO oraz w świetle art. 7 ust. 1–4 ustawy o wspieraniu rodziny i systemie pieczy zastępczej dotyczącego przetwarzania danych osobowych. Przy ocenie omawianego zagadnienia należy brać pod uwagę również konkretne okoliczności faktyczne danego przypadku oraz szczegółowe postanowienia zawarte m.in. w regulaminie organizacyjnym i korzystania z usług danej placówki wsparcia dziennego oraz we wniosku o przyjęcie dziecka do placówki wsparcia dziennego.

KODEKSY POSTĘPOWANIA W OCHRONIE ZDROWIA NA OSTATNIEJ PROSTEJ

Wnioski o udzielenie akredytacji podmiotom monitorującym kodeksy postępowania w ochronie zdrowia, po uzupełnieniu braków formalnych, są obecnie w fazie oceny merytorycznej. Zatem już niedługo możliwe może stać się ich stosowanie w praktyce.

Dotychczas Prezes UODO pozytywnie zaopiniował dwa projekty kodeksów postępowania:

1. projekt Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych (przygotowany przez Federację Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie”) oraz

2. projekt Kodeksu postępowania dla sektora ochrony zdrowia dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających (opracowany przez Polską Federację Szpitali).

Zrobił to jednak z **zastrzeżeniem kwestii monitorowania podmiotów publicznych**, **wskazując, że musi ona zostać doprecyzowana w obu projektach**.

Niezależnie od powyższego, aby kodeksy zostały zatwierdzone, niezbędne jest uzyskanie przez podmioty monitorujące akredytacji Prezesa Urzędu.

Ważna rola podmiotu monitorującego

Podmiot monitorujący pełni ważną rolę w zapewnieniu prawidłowego funkcjonowania kodeksu postępowania. Dlatego musi spełniać określone wymagania, m.in.:

- dysponować odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu,
- zachować niezależność w stosunku do twórców, kandydatów i członków kodeksu oraz przedstawicieli zawodu, branży lub sektora, do których kodeks ma zastosowanie,
- stworzyć procedury i strukturę umożliwiające z jednej strony ocenę, czy administratorzy przestrzegają postanowień kodeksu, a z drugiej skuteczne rozpatrywanie skarg na naruszenia kodeksu.

Organ nadzorczy dokonuje akredytacji podmiotu monitorującego dany kodeks postępowania na podstawie przepisów RODO (art. 41), Wytycznych EROD nr 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących, ustawy o ochronie danych osobowych (art. 27) oraz Wymogów akredytacji podmiotów monitorujących kodeksy postępowania.

Jak się okazuje, ich spełnienie nie jest proste.

W 2021 roku dwa wnioski o udzielenie akredytacji do monitorowania kodeksów postępowania w sektorze ochrony zdrowia zostały pozostawione bez rozpoznania, w związku z nieuzupełnieniem braków formalnych w terminie wskazanym przez organ nadzorczy. Zainteresowane podmioty ponowiły jednak swoje wnioski, a obecnie są już one w fazie oceny merytorycznej. Zakończenie tych postępowań będzie oznaczało możliwość przystąpienia do stosowania kodeksu przez jego pierwszych członków.

Przygotowania warto rozpocząć już teraz

UODO zachęca podmioty medyczne, chcące zapewnić pacjentom wysoki poziom ochrony ich danych osobowych, osiągnięty w projekcie kodeksu przygotowanym przez Polską Federację Szpitali lub też w projekcie kodeksu Porozumienia Zielonogórskiego, by rozpoczęły dostosowywanie się do ich postanowień już teraz. Po ewentualnej akredytacji do zatwierdzonego kodeksu podmiot monitorujący będzie mógł szybko rozpocząć procedurę oceny wstępnej kandydatów na członków tego kodeksu.

Inne inicjatywy

Prace nad kodeksami postępowania w sektorze ochrony zdrowia mogą stanowić przykład i inspirację dla innych branż.

Obecnie Urząd prowadzi postępowania w sprawie jeszcze 6 wniosków o zatwierdzenie kodeksu postępowania w innych branżach i współpracuje z kolejnymi 5 inicjatywami prowadzącymi prace nad projektami kodeksówu. Jednocześnie przygląda się projektom kodeksów transgranicznych, o których mowa w ramach EROD.

Zalety stosowania kodeksu postępowania

Kodeks postępowania, który jest przygotowany zgodnie z przepisami o ochronie danych osobowych, nie jest jedynie powtórzeniem RODO. Kodeks przede wszystkim doprecyzowuje konkretne kwestie związane ze stosowaniem przepisów, uwzględniając specyfikę danej branży. Zatwierdzony kodeks daje wiele korzyści. Ułatwia stosowanie przepisów i wypełnianie nałożonych nimi obowiązków oraz wskazuje właściwe rozwiązania pojawiających się problemów. Zawiera wskazówki pomocne w odpowiednim organizowaniu procesów przetwarzania danych osobowych w danej branży, podnosząc ich poziom. Ten pozytywny aspekt stosowania kodeksu jest odczuwalny zarówno przez administratorów i podmioty przetwarzające, jak i przez osoby, których dane są przetwarzane, gdyż dodatkowo będą one mogły liczyć na podwyższony standard ochrony danych oraz poprawę obsługi w zakresie realizacji ich praw przez daną branżę.

Zatwierdzony kodeks jest nie tylko gwarancją pewności stosowania określonych w nim rozwiązań. Administratorzy mogą także liczyć na nadzór nad procesami przetwarzania danych osobowych przez niezależny podmiot monitorujący kodeks.

KARY

Belgia: upomnienie za brak przejrzystości w sprawie wniosku o usunięcie z listy wyników wyszukiwania

Belgijski organ nadzorczy upomniał jednostkę organizacyjną Google, tj. Google Belgium SA, za nieprzestrzeganie praw osoby, której dane dotyczą.

Decyzja belgijskiego organu ds. ochrony danych osobowych jest następstwem wniosku o usunięcie z listy wyników wyszukiwania kilku artykułów prasowych. W artykułach tych opisano wyroki skazujące byłego adwokata, który w następstwie tych orzeczeń został pozbawiony prawa wykonywania zawodu. Skazania miały miejsce mniej niż 10 lat temu, a skarżący jest obecnie radcą prawnym.

Izba odwoławcza belgijskiego organu nadzorczego oddaliła skargę przeciwko Google za odmowę usunięcia z listy wyników wyszukiwania artykułów prasowych dotyczących skarżącego.

Jednocześnie w tej decyzji (zgodnie z Decyzją 37/2020 belgijskiego organu nadzorczego - decyzja w języku angielskim) przypomniano o kompetencji organu nadzorczego do nakładania kar czy środków naprawczych na lokalną (w tym przypadku belgijską) jednostkę organizacyjną Google (tj. Google Belgium SA), a nie wyłącznie na Google LLC, nawet jeśli jest ona jedynym administratorem danych.

Belgijski organ nadzorczy stwierdził:

- nieprzestrzeganie art. 12 ust. 1 w związku z art. 17 RODO w odniesieniu do jakości uzasadnienia odmowy usunięcia z listy wyników wyszukiwania oraz w odniesieniu do formularza wniosku o usunięcie z listy wyników wyszukiwania poprzez niejasne wskazanie administratora danych;
- nieprzestrzeganie art. 12 ust. 2 w związku z art. 17 RODO w odniesieniu do braku odpowiedniego zapewnienia skarżącemu korzystania z prawa do usunięcia danych, ponieważ skarżący był w rzeczywistości „odsyłany" przez Google Belgium z Google Ireland do Google LLC.

Stwierdzone uchybienia zostały popełnione przez Google LLC, a przypisane Google Belgium, i to do tego podmiotu skierowano upomnienieGoogle Belgium SA. Obecnie toczy się postępowanie odwoławcze od tej decyzji.

Źródło: Decyzja belgijskiego organu

Francja: przedsiębiorstwo ukarane za naruszenie ochrony danych medycznych

Francuski organ nadzorczy (CNIL) uznał, że przedsiębiorstwo Dedalus Biologie nie zastosowało się do przepisów RODO. W rezultacie na tego administratora nałożono administracyjną karę pieniężną w wysokości 1,5 mln euro.

23 lutego 2021 r. prasa ujawniła ogromne naruszenie ochrony danych dotyczące prawie 500 tys. osób. W zdarzeniu uczestniczyło przedsiębiorstwo Dedalus Biologie, które sprzedaje rozwiązania w zakresie oprogramowania dla laboratoriów analiz medycznych. Do Internetu trafiły nazwiska, imiona, numery ubezpieczenia społecznego, nazwiska lekarzy wystawiających receptę, daty badań, ale przede wszystkim informacje medyczne dotyczące stanu zdrowia wielu pacjentów (informacje o przebytych chorobach, np. HIV, nowotwory, choroby genetyczne, ciążach, terapiach lekowych czy dane genetyczne).

CNIL stwierdził trzy naruszenia.

Po pierwsze, w kontekście migracji pakietu oprogramowania na inne narzędzie, o którą poprosiły dwa laboratoria korzystające z usług Dedalus Biologie, to ostatnie pobrało większą ilość danych niż wymagano. Przedsiębiorstwo przetwarzało zatem dane w sposób wykraczający poza polecenia przekazane przez administratorów danych i nie spełniło wymogów art. 29 RODO.

Po drugie, przedsiębiorstwo nie zapewniło bezpieczeństwa danych osobowych w rozumieniu art. 32 RODO. W związku z działalnością Dedalus Biologie stwierdzono liczne naruszenia techniczne i organizacyjne w zakresie bezpieczeństwa w kontekście migracji oprogramowania: brak konkretnej procedury dotyczącej operacji migracji danych; brak szyfrowania danych osobowych przechowywanych na problematycznym serwerze; brak automatycznego usuwania danych po migracji na inne oprogramowanie; brak wymogu uwierzytelnienia z Internetu w celu uzyskania dostępu do publicznej części serwera; korzystanie z kont użytkowników współdzielonych przez kilku pracowników w prywatnej części serwera; brak procedury monitorowania i zgłaszania alarmów bezpieczeństwa na serwerze.

Ten brak odpowiednich środków bezpieczeństwa był jedną z przyczyn naruszenia ochrony danych, które objęło dane medyczne i administracyjne prawie 500 tys. osób. Wreszcie, CNIL ustalił również, że ogólne warunki sprzedaży zaproponowane przez przedsiębiorstwo Dedalus Biologie oraz umowy serwisowe przekazane do CNIL nie zawierały wzmianek przewidzianych w art. 28 ust. 3 RODO.

Źródło: https://edpb.europa.eu/news/national-news/2022/health-data-breach-dedalus-biologie-fined-15-million-euros_en

Holandia: ministerstwo ukarane za nieodpowiednie zabezpieczanie wniosków wizowych

Holenderski organ nadzorczy ukarał holenderskie Ministerstwo Spraw Zagranicznych administracyjną karą pieniężną w wysokości 565 tys. euro za długotrwałe, poważne naruszenia RODO na dużą skalę w procesie wydawania wiz.

Oprócz nałożenia administracyjnej kary pieniężnej, holenderski organ nadzorczy nakazał ministerstwu zapewnienie odpowiedniego poziomu bezpieczeństwa (pod groźbą kary w wysokości 50 tys. euro) oraz zapewnienie osobom ubiegającym się o wizę odpowiednich informacji (pod groźbą kary w wysokości 10 tys. euro). W ciągu ostatnich trzech lat Ministerstwo Spraw Zagranicznych Holandii rozpatrywało średnio 530 tys. wniosków wizowych rocznie. Dane osobowe zawarte we wszystkich tych wnioskach nie są wystarczająco chronione. Dane osobowe, o których mowa, obejmują szczególną kategorię danych osobowych, jak: odciski palców, imię i nazwisko, adres, kraj urodzenia, cel podróży, obywatelstwo i zdjęcie osoby ubiegającej się o wizę.

W ocenie organu nadzorczego Krajowy System Informacji Wizowej (NVIS), czyli system cyfrowy wykorzystywany przez Ministerstwo Spraw Zagranicznych Holandii do obsługi procesu wydawania wiz Schengen, jest nieodpowiednio zabezpieczony. W związku z tym istnieje ryzyko, że osoby nieuprawnione mogą uzyskać dostęp do plików i dokonywać w nich zmian.

Ponadto ministerstwo nie zapewniło osobom ubiegającym się o wizę wystarczających informacji na temat udostępniania ich danych osobowych osobom trzecim.

Źródło: Decyzja holenderskiego organu ws. nałożenia administracyjnej kary na Ministerstwo Spraw Zagranicznych

Holandia: administracja podatkowa ukarana za „czarną listę" oszustw

Holenderski organ nadzorczy nałożył na administrację podatkową karę pieniężną w wysokości 3,7 mln euro za niezgodne z prawem wieloletnie przetwarzanie danych osobowych w ramach „mechanizmu identyfikacji oszustw podatkowych" (FSV).

Będąca przedmiotem dochodzenia Fraude Signalering Voorziening (FSV) była czarną listą, którą administracja podatkowa wykorzystywała do rejestrowania zgłoszeń oszustw, często z poważnymi reperkusjami dla osób, które niesłusznie znalazły się na liście.

Holenderski organ nadzorczy wykrył liczne naruszenia ogólnego rozporządzenia o ochronie danych (RODO). Przede wszystkim administracja podatkowa nie miała podstaw prawnych do przetwarzania danych osobowych znajdujących się na liście.

Co warto podkreślić w wielu przypadkach dane osobowe nie były nawet prawidłowe, w związku z czym osoby były błędnie rejestrowane jako potencjalni sprawcy oszustw podatkowych. Ponadto lista nie była odpowiednio chroniona, a wewnętrzny inspektor ochrony danych w administracji podatkowej na wczesnym etapie tworzenia listy nie został zaangażowany np. do oceny ryzyka.

Źródło: Decyzja holenderskiego organu ws. nałożenia kary na administrację podatkową

EDUKACJA

Raport
„Wiedza na temat bezpieczeństwa danych osobowych w Polsce"

Tegoroczna edycja raportu „Wiedza na temat bezpieczeństwa danych osobowych w Polsce" przedstawia najnowsze wyniki z badania przeprowadzonego przez serwis ChronPESEL.pl i Krajowy Rejestr Długów pod patronatem UODO.

Jak wynika z przeprowadzonego badania 90 proc. Polaków deklaruje, że wie, jak zadbać o bezpieczeństwo swoich danych osobowych. Najpewniej czują się ludzie młodzi. Tylko niewiele ponad połowa (55 proc.) z nas wie, co należy zrobić w przypadku wyłudzenia danych osobowych, takich jak: imię, nazwisko, adres lub numer PESEL. Najwięcej na ten temat wiedzą osoby młode w wieku 18–34 lata, gdzie ten odsetek wynosi około 65 proc.

Ponad 80 proc. ankietowanych sprawę wyłudzenia danych osobowych zgłosiłoby na policję, a blisko 3/4 o zdarzeniu poinformowałoby swój bank. 68 proc. badanych zmieniłoby także hasła do logowania w serwisach, z których korzystają. Ponad 45 proc. ankietowanych zgłosiłoby sprawę do UODO, a blisko co czwarty sprawdziłby w biurze informacji gospodarczej, czy ktoś nie próbował już wykorzystać skradzionych danych.

Pełna treść raportu