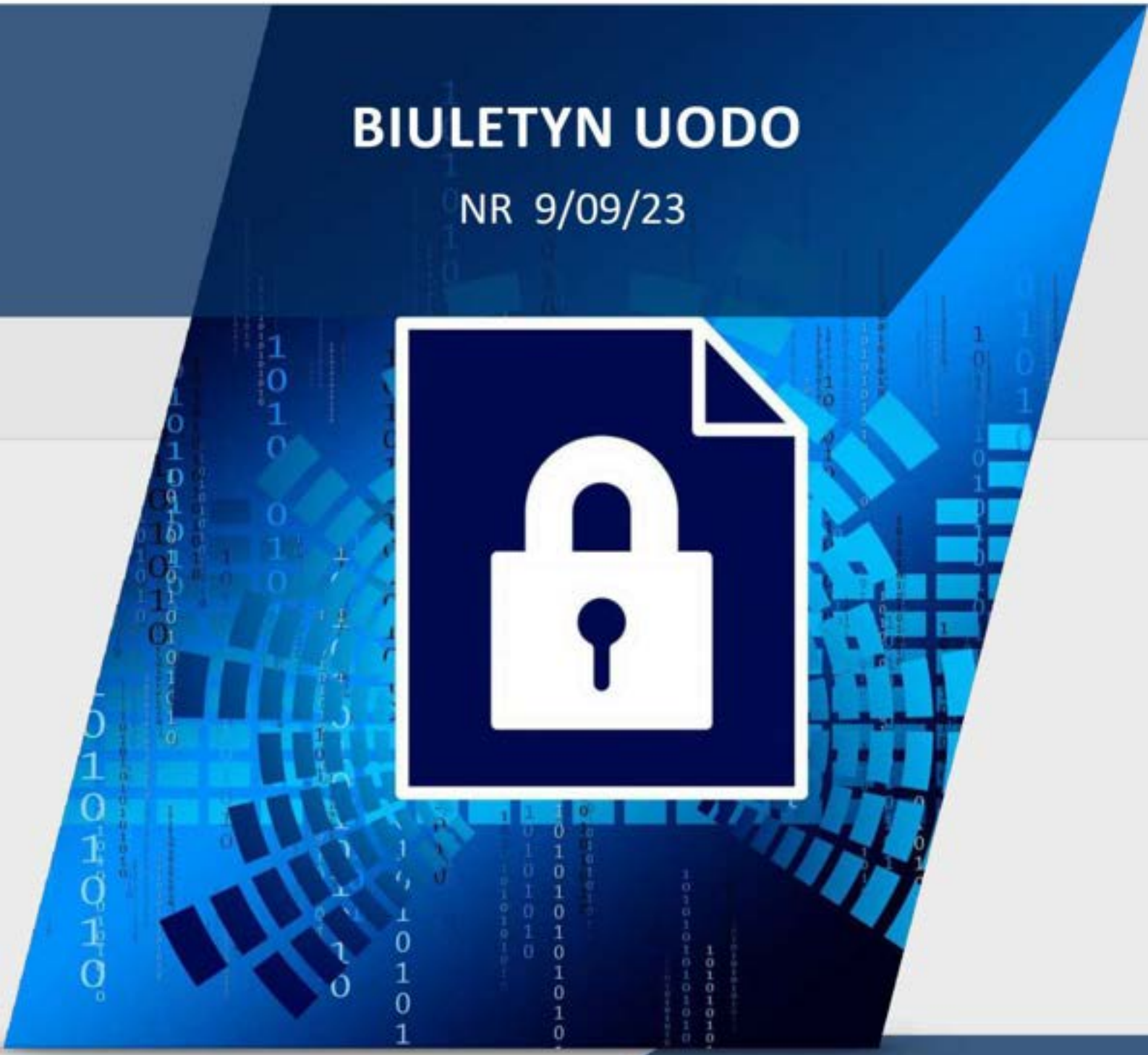
URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO

NR 9/09/23



www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo!

Filozofia ogólnego rozporządzenia o ochronie danych (RODO) wymaga przede wszystkim zapewnienia bezpieczeństwa danych osób fizycznych.
Prezes UODO Jan Nowak wielokrotnie przestrzegał, że utrata kontroli nad danym osobowymi, a więc nad tym, kto i jakie dane o nas przetwarza, może godzić w prawa lub wolność człowieka.
Nadszedł czas, aby przyjrzeć się tej sprawie z perspektywy wyzwań, jakie stawia przed nami postęp technologiczny. Obserwujemy, że w dużej mierze dokonuje się on pod wypływem wykorzystania danych pochodzących z różnych źródeł, w tym danych osobowych, które niejednokrotnie sami udostępniamy. Warto podkreślić, że nie jesteśmy już tylko obserwatorami rozwoju technologicznego, ale wręcz jego aktywnymi uczestnikami i od tego nie ma odwrotu.
Wyzwań związanych z nowoczesnymi technologiami jest wiele, dlatego Urząd Ochrony Danych Osobowych nie tylko bacznie przygląda się nowościom rynkowym i wprowadzaniu kolejnych regulacji w tym zakresie, ale też podejmuje działania związane z monitorowaniem procesów przetwarzania danych osobowych w związku z nowymi technologiami.
Zagadnienia dotyczące relacji pomiędzy ochroną danych osobowych a nowymi technologiami, w tym sztuczną inteligencją, od dawna są przedmiotem zainteresowania polskiego organu ds. ochrony danych m.in. na forum Europejskiej Rady Ochrony Danych.
Jaka przyszłość czeka dane osobowe? Odpowiedzi poszukamy, podejmując dyskusję w gronie ekspertów z rynku krajowego, administracji rządowej czy spółek skarbu państwa podczas wrześniowego Forum Nowych Technologii. Bliżej przyjrzymy się trendom w zakresie usług cyfrowych czy cyberbezpieczeństwa, a dwudniowa konferencja to okazja, aby w czasie sesji tematycznych oraz debat omówić wiele istotnych zagadnień. Przykładowo poruszymy zagadnienia: jak rozwijać ochronę danych osobowych w erze nowych technologii, jakie wyzwania prawne z zakresu ochrony danych osobowych i etyczne wiążą się z wykorzystaniem sztucznej inteligencji, czy jesteśmy gotowi zapewnić bezpieczeństwo informacji w erze cyfrowej, z jakimi wyzwaniami w erze innowacji będą mierzyć się organy nadzorcze. Podyskutujemy także o wyzwaniach w legislacji, w związku z nowym prawem unijnym i krajowym. Już dzisiaj zapraszamy wszystkich Państwa do udziału w Forum Nowych Technologii, które odbędzie się 20 i 21 września. Weźmie w nim udział ok. 40 wybitnych ekspertów w sześciu sesjach tematycznych. Po szczegóły zapraszam na stronę uodo.gov.pl

Jakub Groszkowski
Zastępca Prezesa UODO

Drodzy Czytelnicy!

Edukacja zajmuje szczególne miejsce w działalności Urzędu Ochrony Danych Osobowych, dlatego wrzesień dla pracowników UODO jest miesiącem wyjątkowym. To czas, w którym zaczynamy nabór do prowadzonego od lat z sukcesem programu edukacyjnego dla szkół i uczniów „Twoje Dane – Twoja Sprawa". Jesteśmy dumni, że przyczyniamy się do budowania wśród najmłodszych pozytywnych nawyków ochrony danych osobowych i prawa do prywatności. W tym roku zakończyliśmy także pierwszą edycję „Letniej Akademii Liderów RODO", nowej inicjatywy UODO dla studentów i absolwentów wzbogacającą ich o praktyczną wiedzę na temat zasad ochrony danych osobowych. Uczestnikom serdecznie gratulujemy i cieszymy się, że bierzemy udział w wykształceniu nowego pokolenia liderów RODO.

W obecnym numerze Biuletynu poświęcamy edukacji dodatkowe miejsce. Programy studiów związane z ochroną danych osobowych stanowią wartościową inwestycję w przyszłość. Dają one możliwość zdobycia kompleksowej wiedzy i umiejętności niezbędnych w dzisiejszym cyfrowym świecie, a także otwierają drzwi do różnorodnych ścieżek kariery zawodowej. Ochrona danych staje się coraz ważniejsza, dlatego też coraz więcej osób decyduje się na podjęcie takich studiów, aby być przygotowanym do wyzwań związanych z zarządzaniem bezpieczeństwem informacji i ochroną prywatności. Zapraszam do lektury wywiadu na temat kluczowych aspektów programów studiów z zakresu ochrony danych osobowych z Prof. dr hab. Jerzym Pisulińskim, Dziekanem Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego, a także obszernego komentarza mgr Sławomira Jagieły EMBA, DBA. Dyrektora Kolegium Kształcenia Podyplomowego Akademii Ekonomiczno-Humanistycznej w Warszawie.

W każdym numerze „Biuletynu UODO" stajemy przez wyzwaniami związanymi z ciągłym rozwojem nowych technologii. Tym razem przybliżamy czytelnikom temat zwodniczych interfejsów w sektorze cyfrowym. Mowa oczywiście o dark patterns. Czym są te szkodliwe praktyki, które mogą naruszać nie tylko przepisy RODO i przepisy o ochronie konsumentów, ale również akt o usługach cyfrowych (DSA) i jak się przed nimi chronić? Odpowiedzi na te i inne pytania można znaleźć w dziale „Nowe technologie". Z kolei Dyrektor Departamentu Polityki Konsumenckiej z Urzędu Komunikacji Elektronicznej, Dorota Grudzień-Barbachowska przedstawia wyniki rokrocznie prowadzonych przez UKE badań i analiz prezentujących sposób, w jaki Polacy korzystają z Internetu w dobie komunikacji elektronicznej. Polecamy przyjrzeć się tej ciekawej lekturze.

W najnowszym wydaniu piszemy także o tym, że Komisja Europejska zaproponowała nowe przepisy mające usprawnić współpracę między organami ochrony danych podczas egzekwowania ogólnego rozporządzenia o ochronie danych (RODO) w sprawach transgranicznych.

Zmiany obserwujemy też po drugiej stronie globu. Po sześciu latach starań, Indie przyjęły ustawę o ochronie przetwarzanych danych osobowych. To skutek jednego z wyroków Sądu Najwyższego Indii, który uznał prywatność za prawo podstawowe.

Wrześniowe wydanie „Biuletynu UODO" zawiera również ważne wskazówki dla administratorów. Urząd podpowiada co powinni zrobić, gdy potrzebują więcej niż 72 godziny od stwierdzenia naruszenia na zgromadzenie informacji niezbędnych do dokonania prawidłowego zgłoszenia. Materiał ten z pewnością rozjaśni tę niezwykle istotną dla administratorów kwestię.
Last but not least – bardzo ważny temat, rozmowa z ekspertem numeru o tym dlaczego liczba skarg składanych do Prezesa UODO rośnie z roku na rok, o oczekiwaniach skarżących wobec Urzędu, dlaczego rozstrzygnięcie skargi wymaga czasu oraz o tym, jakie elementy skarga musi koniecznie zawierać, aby Prezes UODO mógł ją rozpatrzeć dowiecie się z rozmowy z Pauliną Dawidczyk, Dyrektorką Departamentu Skarg w UODO.

Jestem przekonany, że najnowszy numer „Biuletynu UODO" to duża dawka potrzebnej wiedzy na temat ochrony danych osobowych. Pozostaje mi życzyć czytelnikom miłej lektury!

Adam Sanocki
Dyrektor Departamentu Komunikacji Społecznej, Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

ZANIM ZŁOŻYMY SKARGĘ DO PREZESA UODO, ZGŁASZAJMY SWOJE ŻĄDANIA ADMINISTRATOROWI

Paulina Dawidczyk, Dyrektor Departamentu Skarg na temat procesu rozpatrywania skarg przez organ nadzorczy rozmawia z Adamem Sanockim.

Osoby, które uważają, że poprzez np. ujawnienie ich danych osobowych naruszone zostało ich prawo do ochrony tych danych, mogą złożyć skargę do Prezesa UODO[1]. Biorąc pod uwagę, że liczba skarg gwałtownie wzrosła po rozpoczęciu stosowania RODO i nadal jest wysoka, czy możemy wskazać czynniki, które miały na to wpływ?

Faktycznie liczba skarg składanych do Prezesa UODO rośnie z roku na rok. Większy ich wpływ do UODO świadczy m.in. o wzroście świadomości obywateli co do przysługujących im praw w zakresie ochrony prywatności i danych osobowych. I trzeba przyznać, że skarżący nieustannie wykazują duże zainteresowanie dochodzeniem swoich praw z zakresu ochrony danych osobowych. Obecnie ta procedura nie wiąże się z dodatkowymi opłatami, co także czyni ją bardziej dostępną.

Dynamikę tego procesu najłatwiej zilustrować liczbami. W 2018 roku do organu nadzorczego wpłynęło 5565 skarg, z czego zdecydowana większość, tj. 4550 w okresie od 25 maja do 31 grudnia 2018 r., a więc już po rozpoczęciu stosowania wówczas nowych przepisów – RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. W kolejnych latach zauważalny był dalszy skokowy wzrost skarg (patrz Wykres). Dla porównania warto przypomnieć, że przed rokiem 2018 ta liczba nie przekraczała nawet 3 tysięcy.

Ponadto dane porównawcze z lat poprzednich – co warto podkreślić – wykazują, że liczba wydawanych przez Prezesa UODO decyzji administracyjnych, w sprawach zainicjowanych skargami osób, których dane dotyczą, stale wzrasta, pomimo utrzymującego się wysokiego poziomu wpływu nowych skarg.

ROK	ŁĄCZNA LICZBA ZŁOŻONYCH SKARG
2018	5565
2019	9304
2020	6442
2021	8318
2022	6995

1 ROZMOWA Z EKSPERTEM

W 2022 roku do Prezesa UODO wpłynęło aż 6995 skarg osób, których dane dotyczą na przetwarzanie ich danych, zaś wskazywana liczba 86 orzeczeń zapadła w sprawach, które stanowią 1,3% z ww. liczby skarg.

Czy to oznacza, że efektywność organu wzrasta?

Tak, wbrew wskazywanym w mediach twierdzeniom efektywność organu w sprawach skargowych wzrosła. W roku 2022 aż 1830 spraw skargowych zakończyło się wydaniem decyzji administracyjnej. W 2021 roku wydaniem decyzji administracyjnej zakończyły się 1734 sprawy, zaś w roku 2020 – było to 1401 spraw. Podkreślić należy, że każdemu, kto jest stroną postępowania administracyjnego przysługuje prawo do złożenia skargi na przewlekłe prowadzenie postępowania czy też bezczynność. Należy jednak wziąć pod uwagę to, że nie zawsze taka skarga jest zasadna. Podkreślić trzeba, że w dużej liczbie spraw, w których wpłynęła skarga na przewlekłość sądy administracyjne oddalają skargę lub ją odrzucają. Zauważyć należy także, że im więcej spraw rozpatruje organ, tym naturalnie więcej jest także skarg na przewlekłość i bezczynność organu, co nie znaczy, że każda taka skarga jest zasadna.

Odnosząc się do wskazywanej w mediach liczby 86 orzeczeń sądów w sprawach dotyczących bezczynności w 2022 roku, należy zauważyć, że jak wynika z orzeczeń doręczonych do organu, w 2022 roku sądy administracyjne skargę na przewlekłość uwzględniły jedynie w 13 przypadkach. Dodatkowo nie we wszystkich przypadkach organ podzielił stanowisko sądu, wobec czego wniósł skargę kasacyjną, zatem nie wszystkie z 13 orzeczeń są prawomocne. To te dane należy przede wszystkim uwzględnić oceniając efektywność organu.

W 2022 roku do Prezesa UODO wpłynęło aż 6995 skarg osób, których dane dotyczą na przetwarzanie ich danych, zaś wskazywana liczba 86 orzeczeń zapadła w sprawach, które stanowią 1,3% z ww. liczby skarg. Natomiast liczba doręczonych do organu orzeczeń uwzględniających skargę na przewlekłość stanowi 0,2% z ww. liczby skarg osób, których dane dotyczą na przetwarzanie ich danych. Dopiero uwzględniając powyższe informacje można mówić o tym, jak przedstawia się efektywność organu nadzorczego w rozpatrywaniu skarg.

Proszę przybliżyć czytelnikom „Biuletynu UODO", jakich kwestii skargi dotyczą najczęściej?

Powody są bardzo zróżnicowane. Osoby, których dane dotyczą, często skarżą się na przetwarzanie ich danych osobowych bez podstawy prawnej, w tym na ich udostępnienie podmiotom nieuprawnionym oraz niechciane działania marketingowe z wykorzystaniem ich danych. Duża część skarg dotyczy także niespełnienia obowiązków informacyjnych wynikających z RODO, w tym nieprzekazania kopii danych, zgodnie z art. 15 ust. 3 RODO. Odnotowaliśmy także liczne skargi na nieprawidłowe wykonanie obowiązku sprostowania danych oraz nieprawidłową realizację prawa do usunięcia danych wynikającego z art. 17 RODO i prawa sprzeciwu, o którym mowa w art. 21 RODO.

1 ROZMOWA Z EKSPERTEM

Z obserwacji organu nadzorczego wynika, że często skarżący wskazują także na naruszenie ochrony danych osobowych osób trzecich, jak również składają skargi dotyczące przyszłego przetwarzania, które nie zaistniało na dzień złożenia skargi.

Wiele ciekawych informacji dostarcza także analiza skarg pod kątem sektorów. Czy tu także może Pani wskazać jakieś konkretne powody?

Tak. Przykładowo, w sektorze publicznym najczęstszymi powodami skarg są takie zdarzenia, jak udostępnianie danych osobowych: na stronach internetowych (np. w Biuletynie Informacji Publicznej, na oficjalnej stronie internetowej prowadzonej przez organ, na portalu społecznościowym) czy podczas obrad kolegialnych organów jednostek samorządu terytorialnego, w tym w związku z transmisją i nagrywaniem obrad kolegialnych tych organów. Ponadto skarżący sygnalizują, że dochodzi do udostępnienia danych osobowych osobom trzecim/podmiotom trzecim (np. poprzez przesłanie korespondencji do niewłaściwego adresata, umożliwienie wglądu w akta sprawy osobie nieuprawnionej) albo osoby zawiadamiającej o nieprawidłowościach (sygnalisty) czy osadzonych na rzecz innych osadzonych przez funkcjonariuszy służby więziennej. Wciąż zdarzają się skargi na udostępnienia danych osobowych osobom trzecim poprzez brak ukrycia adresu e-mail w polu „do wiadomości" lub udostępniania osobom trzecim/podmiotom trzecim danych osobowych z rejestrów prowadzonych przez organ.

Z kolei w sektorach zdrowia, zatrudnienia i szkolnictwa skargi najczęściej odnoszą się do kwestii dotyczących przetwarzania lub udostępnienia danych osobowych bez podstawy prawnej.

Natomiast w sektorze prywatnym skargi najczęściej dotyczą nieprawidłowości w procesie przetwarzania danych osobowych w celach marketingowych, w tym utrudniania przez administratora danych realizacji przez podmiot danych przysługujących mu na mocy RODO praw, a także przetwarzania danych osobowych w zakresie wizerunku utrwalonego za pomocą monitoringu wizyjnego oraz udostępnienia danych osobowych podmiotom nieuprawnionym.

W przypadku sektora finansowego do najczęściej zgłaszanych nieprawidłowości wciąż należy przetwarzanie danych osobowych przez banki w związku z zapytaniami kredytowymi, które nie zakończyły się zawarciem umowy oraz przetwarzaniem danych osobowych w oparciu o art. 105a ust. 3 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe pomimo niespełnienia warunków określonych w tym przepisie.

Z obserwacji organu nadzorczego wynika, że często skarżący wskazują także na naruszenie ochrony danych osobowych osób trzecich, jak również składają skargi dotyczące przyszłego przetwarzania, które nie zaistniało na dzień złożenia skargi.

Ponadto skarżący oczekują od organu nie tylko badania legalności procesów przetwarzania ich danych, przetwarzania danych zgodnie z zasadami wykonywania operacji na danych czy weryfikacji spełniania obowiązków informacyjnych z art. 13, art. 14 oraz 15 RODO. Skarżący chcą także – często nie podejmując w pierwszej kolejności stosownych działań przed administratorem – aby organ nadzorczy wyręczył ich w realizacji ich praw z art. 15–22 RODO. Takie żądania skarżący składają, zwłaszcza gdy kontakt z administratorem jest dla nich utrudniony.

Ponadto wyjątkowo liczne są również skargi na odmowę realizacji prawa osoby skarżącej do bycia zapomnianym (art. 17 RODO) przez administratora będącego aktualnym wierzycielem osoby skarżącej, który nabył wierzytelność w drodze umowy cesji.

1 ROZMOWA Z EKSPERTEM

UODO jest organem właściwym wyłącznie w sprawach ochrony danych osobowych i w związku z tym nie posiada kompetencji m.in. do orzekania w sprawach z zakresu ochrony dóbr osobistych

Do UODO często wpływają także skargi dotyczące naruszenia ochrony danych osobowych związane z tzw. „wyciekiem danych", w których skarżący po otrzymaniu od administratora danych zawiadomienia o zaistniałym naruszeniu, oczekiwali od Prezesa UODO zabezpieczenia ich przed konsekwencjami tego naruszenia. W tym miejscu warte odnotowania jest to, że Prezes UODO nie jest władny do zabezpieczenia takich osób przed ewentualnymi negatywnymi skutkami nieprawidłowości w zakresie przetwarzania ich danych osobowych.

Czy to oznacza, że skarżący oczekują więcej niż faktycznie przewidują uprawnienia organu nadzorczego?

Wiele osób składających skargi i formułując swoje żądania wobec organu często nie ma świadomości, że Prezes UODO jest organem właściwym wyłącznie w sprawach ochrony danych osobowych i w związku z tym nie posiada kompetencji m.in. do orzekania w sprawach z zakresu ochrony dóbr osobistych (np. wizerunku, prawa do prywatności), nakazania wypłaty odszkodowania czy zadośćuczynienia czy orzekania w kwestii oceny warunków, skuteczności czy też ważności umów cywilnoprawnych.

Biorąc pod uwagę zwiększającą się świadomość społeczną w kontekście praw dotyczących ochrony danych osobowych, należałoby zachęcać skarżących, aby w pierwszej kolejności samodzielnie zwracali się do podmiotów, które ich zdaniem nie przestrzegają powszechnie obowiązujących przepisów, a dopiero potem kierowali skargi z właściwymi żądaniami do Prezesa UODO.

Skarżący powinni mieć również na uwadze, że nakładanie administracyjnych kar pieniężnych należy do uprawnień Prezesa UODO niezależnych od żądania osoby składającej skargę, jak również – w aspekcie przedwczesności zgłaszanych skarg do organu nadzorczego – pamiętać powinni o przysługujących administratorowi terminach, w których zobowiązany jest on wywiązać się ze swoich obowiązków i spełnić ich żądania.

Skarżący powinni mieć również na uwadze, że nakładanie administracyjnych kar pieniężnych należy do uprawnień Prezesa UODO niezależnych od żądania osoby składającej skargę

1 ROZMOWA Z EKSPERTEM

Skorzystaj ze swoich praw, zanim złożysz skargę do Prezesa UODO

Administrator ma obowiązek najszybciej jak to możliwe odpowiedzieć na Twoje żądanie – maksymalnie w terminie miesiąca. Jeżeli z jakiegoś powodu nie będzie to możliwe, musi Cię poinformować, dlaczego przedłuża termin odpowiedzi o nieprzekraczalne kolejne dwa miesiące. Także w ciągu miesiąca administrator powinien Cię poinformować o niespełnieniu żądania i jego przyczynach. Jeżeli administrator zignoruje Twoje żądanie albo odpowiedź nie będzie dla Ciebie satysfakcjonująca możesz złożyć skargę do Urzędu. Niezależnie od postępowania przez UODO masz prawo do ochrony swoich praw przed sądem cywilnym. Jeżeli uznasz, że przetwarzanie Twoich danych osobowych narusza przepisy prawa, możesz pozwać administratora lub podmiot przetwarzający. Przed sądem możesz żądać odszkodowania za naruszenie przepisów o ochronie danych osobowych, które spowodowało szkodę majątkową lub niemajątkową. Ta kwestia może być rozstrzygnięta wyłącznie przed sądem powszechnym. W postępowaniu przed Prezesem Urzędu nie można tego uczynić.

A na jakie trudności natrafiają eksperci UODO, gdy analizują sprawy w postępowaniach skargowych?

Każda ze skarg analizowana jest pod kątem spełnienia warunków formalnych przewidzianych przepisami Kodeksu postępowania administracyjnego (dalej: k.p.a.). Szczególnie podkreślić trzeba, że Prezes UODO nie rozpatruje skarg anonimowych, a te zdarzają się często. Brak informacji identyfikujących skarżącego, a także danych adresowych spowoduje, że skarga nie zostanie rozpatrzona z uwagi na brak możliwości kontaktu. Równie często skarżący popełniają błędy w zakresie wymogów formalnych w składanych przez nich pismach. W sytuacji gdy skarga nie spełnia warunków wymaganych przez k.p.a., organ ochrony danych wzywa wnioskodawcę do ich usunięcia we wskazanym terminie. Niestety, sprawy, w których nie zostaną usunięte braki formalne, także pozostaną bez rozpoznania. Najczęściej skarżący wzywani są do doprecyzowania żądania mieszczącego się w zakresie kompetencji przysługujących Prezesowi UODO, gdyż większość z nich wnosi m.in. o samo wszczęcie postępowania w sprawie, nie wskazując podjęcia jakich działań w sprawie domagają się od Prezesa UODO.

Najczęściej skarżący wzywani są do doprecyzowania żądania mieszczącego się w zakresie kompetencji przysługujących Prezesowi UODO, gdyż większość z nich wnosi m.in. o samo wszczęcie postępowania w sprawie, nie wskazując podjęcia jakich działań w sprawie domagają się od Prezesa UODO.

1 ROZMOWA Z EKSPERTEM

Skarżący zostają także zobligowani do przedstawienia bardziej precyzyjnego opisu stanu faktycznego sprawy m.in. w zakresie wskazania danych, których dotyczy naruszenie i określenia na czym ono polega.

Skarżący wnoszą o: stwierdzenie, czy doszło do naruszenia ich prawa do ochrony danych osobowych, o przeprowadzenie kontroli w stosunku do skarżonego podmiotu, o nałożenie administracyjnej kary pieniężnej oraz o ustalenie podmiotu, który dopuszcza się naruszenia ich prawa do ochrony danych osobowych, a także wypłaty odszkodowania/zadośćuczynienia. Ponadto wnioskodawcy wzywani są do wskazania pełnej nazwy oraz adresu siedziby albo imienia, nazwiska oraz adresu skarżonego podmiotu oraz do wskazania swojego adresu poczty tradycyjnej, w szczególności, gdy podanie jest wnoszone przez skarżących za pomocą środków komunikacji elektronicznej (ePUAP), gdyż błędnie przyjmują, że samo podpisanie podania (kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym) powinno pozwolić zindywidualizować ich jako strony postępowania. Skarżący zostają także zobligowani do przedstawienia bardziej precyzyjnego opisu stanu faktycznego sprawy m.in. w zakresie wskazania danych, których dotyczy naruszenie i określenia na czym ono polega. W przypadku spraw dotyczących naruszenia ochrony danych osobowych w Internecie, skarżący wzywani są do podania administratorów i linków stron internetowych.

7 typowych braków formalnych, bez uzupełnienia których skarga nie będzie rozpatrzona

1. Brak wskazania z imienia i nazwiska skarżącego oraz adresu poczty tradycyjnej;
2. Brak złożenia podpisu własnoręcznego lub elektronicznego
3. Brak wskazania konkretnych lub prawidłowo sformułowanych żądań, wynikających z przepisów RODO;
4. Brak określenia podmiotu skarżącego, którego podanie jest niezbędne do wszczęcia postępowania administracyjnego;
5. Składanie skarg do UODO na formularzach przeznaczonych do zgłaszania Prezesowi Urzędu Ochrony Danych Osobowych naruszeń ochrony danych osobowych.
6. Składanie skarg w niedozwolonej prawnie formie (tj. w formie e-mail).
7. Ponadto w sytuacji, gdy zgłaszane naruszenie dotyczyło także innej osoby skarżący często nie dołączali pełnomocnictwa do występowania w jej imieniu, co w efekcie i mimo wezwania mogło uniemożliwiać rozpatrzenie podania wobec tej osoby.

1 ROZMOWA Z EKSPERTEM

Jeżeli przedmiotem skargi jest sam fakt udostępnienia danych osobowych podmiotom nieuprawnionym, nie ma konieczności wskazywania żądania. W takim przypadku wystarczy wskazać, że kwestionuje się udostępnienie danych przez administratora innemu podmiotowi.

Zatem przypomnijmy, jakie elementy skarga musi koniecznie zawierać, aby Prezes UODO mógł ją rozpatrzeć.

Rozpocznijmy od kwestii fundamentalnej. Każda skarga złożona do Prezesa Urzędu musi zawierać pięć elementów:

1. imię i nazwisko oraz adres zamieszkania osoby skarżącej;
2. wskazanie podmiotu, na który osoba, której dane dotyczą, składa skargę (nazwa/imię i nazwisko oraz adres siedziby/zamieszkania);
3. dokładny opis naruszenia;
4. żądanie skarżącego – jakich działań oczekuje od Prezesa UODO (np. usunięcia danych, wypełnienia obowiązku informacyjnego, sprostowania danych, ograniczenia przetwarzania danych itd.)
5. własnoręczny podpis;

Istnieją jeszcze inne elementy, które mają istotny wpływ na to, co będzie działo się ze skargą. Jeżeli zgłaszana skarga zawiera więcej niż jedno żądanie, należy zwrócić uwagę, by nie były one ze sobą sprzeczne (np. nie można żądać, aby podmiot, którego działalność się skarży, wykonał obowiązek informacyjny i jednocześnie żądać, by podmiot ten usunął dane osobowe).

Jeżeli przedmiotem skargi jest sam fakt udostępnienia danych osobowych podmiotom nieuprawnionym, nie ma konieczności wskazywania żądania. W takim przypadku wystarczy wskazać, że kwestionuje się udostępnienie danych przez administratora innemu podmiotowi.

Skarżący powinni pamiętać, by dołączyć dowody potwierdzające nieprawidłowe działanie administratora (np. korespondencję z administratorem, umowy, zaświadczenia). Ułatwi to pracownikom Urzędu ocenę.

Skargi można składać w formie pisemnej, w tym ustnie do protokołu w siedzibie Urzędu po wcześniejszym umówieniu na konkretną godzinę, lub elektronicznej. W tym drugim przypadku kierowanie skargi następuje przez Elektroniczną Skrzynkę Podawczą Prezesa Urzędu (skarżący wypełnia formularz w postaci „Pismo ogólne do podmiotu publicznego" dostępny na portalu ePUAP2). Skarga składana w formie elektronicznej, oprócz wymogów dla skargi w formie pisemnej, musi być opatrzona kwalifikowanym podpisem elektronicznym albo podpisem zaufanym, albo podpisem osobistym, lub uwierzytelniona w sposób zapewniający możliwość potwierdzenia pochodzenia i integralności weryfikowanych danych w postaci elektronicznej, zawierać adres elektroniczny skarżącego.

Zdajemy sobie sprawę, że ochrona danych osobowych i ochrona prywatności są szczególnie ważne w kontekście przetwarzania ogromnej liczby informacji przez zaawansowane systemy informatyczne. Dlatego UODO przygląda się temu zagadnieniu w trosce o ochronę danych osobowych obywateli.

Aby kształcić młode pokolenie, świadome swoich praw i obowiązków pod względem ochrony danych osobowych, trzeba docierać z wiedzą na ten temat do dyrektorów szkół, nauczycieli i rodziców. Cele te są realizowane przez program „Twoje dane – Twoja sprawa".

W tym kontekście wyjaśnienia wymaga także zagadnienie czasu rozstrzygnięcia skarg złożonych do Urzędu. Czy może Pani wytłumaczyć, jak Urząd załatwia takiego typu sprawy?

Dla czytelnika, który niezawodowo zajmuje się ochroną danych osobowych, może się wydawać oczywiste, że gdy wpłynie skarga, urząd zamknie sprawę w ciągu miesiąca. Gdy jednak przyjrzymy się uważnie przepisom, które regulują tę sferę funkcjonowania administracji, to okazuje się, że sprawa jest bardziej złożona. Zgodnie z przepisami art. 35 § 3 k.p.a. organ ma miesiąc na załatwienie sprawy wymagającej postępowania wyjaśniającego, a w przypadkach szczególnie skomplikowanych termin ten wynosi dwa miesiące. Przestrzeganie tych terminów jest jednak trudne do skutecznej realizacji. Na wydłużenie czasu postępowań wpływa stopień skomplikowania oraz indywidualny charakter każdej sprawy, konieczność uzyskania wyczerpujących wyjaśnień, tak by zebrać stosowny materiał dowodowy w sprawie, będący podstawą wydania rozstrzygnięcia oraz uwzględnienia wszystkich aspektów sprawy. Dla długości prowadzonego postępowania mają także znaczenie kwestie związane z mniej lub bardziej udaną współpracą z administratorami i skarżącymi. Odnosząc się do kwestii czasu rozstrzygnięcia skarg, trzeba też pamiętać, że postępowanie przed Prezesem UODO cechuje określona specyfika. Przykładowo, UODO jest jedynym urzędem w Polsce, bez jednostek pomocniczych czy oddziałów zamiejscowych. Tymczasem wnoszone skargi mają coraz bardziej skomplikowany charakter i wymagają zwiększonej ilości czasu przeznaczanego na ich rozpatrzenie, co znacznie wydłuża okresy prowadzonych postępowań administracyjnych.

Dziękuję za rozmowę.

PRZYPISY

[1] Postępowanie wszczęte przez Prezesa UODO z urzędu lub na wniosek osoby zainteresowanej dotyczące naruszenia przepisów o ochronie danych osobowych toczą się zgodnie z normami proceduralnymi określonymi przepisami ustawy z 10 maja 2018 r. o ochronie danych osobowych, a w zakresie w tej ustawie nieuregulowanym, przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego30. W przypadku stwierdzenia naruszenia przepisów prawa, postępowanie to może zakończyć się wydaniem decyzji administracyjnej nakazującej administratorowi danych określone zachowanie lub nałożeniem administracyjnej kary pieniężnej. Pomimo autonomii proceduralnej państw członkowskich UE pewne kwestie proceduralne, zwłaszcza związane z postępowaniami transgranicznymi zostały bezpośrednio uregulowane w RODO.

[2] Dz. U. z 2021 r. poz. 2439 z późn. zm.

2 UODO SYGNALIZUJE

NIEUPRAWNIONE KONTAKTOWANIE SIĘ PRZEDSTAWICIELI SZKOŁY Z LEKARZEM BADAJĄCYM UCZNIA

Pracownik placówki dydaktycznej nie jest uprawniony do omawiania stanu zdrowia ucznia odbywającego praktyczną naukę zawodu z lekarzem przeprowadzającym badanie.

Z prośbą o wyjaśnienie wątpliwości w tym zakresie zwróciła się do UODO matka pewnego ucznia technikum, który odbywał praktyczną naukę zawodu. Szczegółowo opisała sytuację, w której dyrektor tej szkoły bez zgody rodziców kontaktował się z lekarzem medycyny pracy przeprowadzającym badanie ucznia. Matka spytała UODO, czy jakiekolwiek osoby postronne, w tym dyrektor szkoły, mają prawo kontaktować się z lekarzem i dyskutować o zdrowiu pacjenta lub też przekazywać pisemne opinie bez zawiadomienia rodziców o ich wydaniu.

W odpowiedzi organ nadzorczy wskazał, że przetwarzanie danych osobowych uczniów, którzy narażeni są na działanie czynników szkodliwych, uciążliwych lub niebezpiecznych dla zdrowia regulują przepisy rozporządzenia Ministra Zdrowia z dnia 26 sierpnia 2019 r. w sprawie badań lekarskich kandydatów do szkół ponadpodstawowych lub wyższych i na kwalifikacyjne kursy zawodowe, uczniów i słuchaczy tych szkół, studentów, słuchaczy kwalifikacyjnych kursów zawodowych oraz doktorantów, wydanego na podstawie delegacji zawartej w art. 6 ust. 5 ustawy z dnia 27 czerwca 1997 r. o służbie medycyny pracy.

Zgodnie z § 3 ust. 1 tego rozporządzenia lekarz przeprowadza badanie lekarskie na podstawie skierowania wydanego przez placówkę dydaktyczną. Z kolei zaświadczenie lekarskie wydawane jest w dwóch egzemplarzach, z których jeden pozostaje w dokumentacji lekarskiej, natomiast drugi przekazywany jest osobie badanej (posiadającej pełną zdolność do czynności prawnej lub przedstawicielowi ustawowemu, gdy jej nie posiada) w celu przekazania placówce dydaktycznej kierującej na badanie.

2 UODO SYGNALIZUJE

Zarówno uczniowi, jak i placówce dydaktycznej przysługuje wnoszone na piśmie odwołanie od orzeczenia o istnieniu lub braku przeciwskazań zdrowotnych do wykonywania zawodu i odbywania praktycznej nauki zawodu. Z przepisów rozporządzenia nie płyną jednak prerogatywy upoważniające pracownika placówki dydaktycznej do omawiania stanu zdrowia ucznia z lekarzem przeprowadzającym badanie lekarskie. Informacje związane z udzielanym świadczeniem zdrowotnym zaliczane są do szczególnych kategorii danych osobowych, o których mowa w art. 9 RODO, i których przetwarzanie jest co do zasady zabronione.

Chcąc przetwarzać dane o stanie zdrowia należy wykazać się jedną z przesłanek określonych w art. 9 ust. 2 RODO dopuszczających przetwarzanie tej kategorii danych. Wśród nich wymienić można m.in.: wyrażenie przez osobę, której dane dotyczą, wyraźnej zgody na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach; zaistnienie sytuacji, w której przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą; przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody. Przesłanki te odwołują się dodatkowo do odpowiednich gwarancji, co oznacza, że przetwarzanie szczególnych kategorii danych osobowych jest dopuszczalne wyłącznie w ściśle określonych okolicznościach.

POZYSKIWANIE NUMERU PESEL OD NAUCZYCIELA SKAŁADAJĄCEGO WNIOSEK O PODJĘCIE POSTĘPOWANIA EGZAMINACYJNEGO LUB KWALIFIKACYJNEGO

Organ prowadzący szkołę nie ma podstawy prawnej do żądania od nauczyciela ujawnienia we wniosku o podjęcie postępowania egzaminacyjnego lub postępowania kwalifikacyjnego jego numeru PESEL.

Przepisy ustawy z dnia 26 stycznia 1982 r. Karta Nauczyciela przewidują (art. 9b ust. 2a), że wniosek o podjęcie postępowania egzaminacyjnego lub postępowania kwalifikacyjnego zawiera: imię (imiona) i nazwisko, datę urodzenia oraz adres do korespondencji nauczyciela; miejsce zatrudnienia i zajmowane stanowisko; podpis nauczyciela. Stosownie zaś do art. 9b ust. 2b do wniosku o podjęcie postępowania egzaminacyjnego lub postępowania kwalifikacyjnego dołącza się oryginały lub kopie dokumentów potwierdzających spełnianie warunków niezbędnych do uzyskania stopnia awansu zawodowego, o których mowa w ust. 1 pkt 1-4, ust. 1a pkt 1-3 oraz ust. 1c, a w przypadku wniosku o podjęcie postępowania kwalifikacyjnego – także opis i analizę sposobu spełniania wymagań dotyczących realizowania zadań lub podejmowania działań na rzecz oświaty oraz ich efektów, określonych w przepisach wydanych na podstawie art. 9g ust. 10.
Zatem w katalogu danych koniecznych do złożenia wniosku o podjęcie postępowania egzaminacyjnego lub postępowania kwalifikacyjnego ustawodawca nie przewidział pozyskiwania numeru PESEL nauczyciela.
Wskazać jednak należy, że przepisy ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej wymagają pozyskania numeru PESEL nauczyciela do bazy Systemu Informacji Oświatowej (SIO). Zgodnie bowiem z art. 27 tej ustawy w bazie danych SIO, w zbiorach danych nauczycieli, są gromadzone i przetwarzane dane identyfikacyjne i dane dziedzinowe nauczycieli. Natomiast dane identyfikacyjne nauczyciela obejmują imię, nazwisko i numer PESEL, a w przypadku nauczyciela nieposiadającego numeru PESEL – imię (imiona), nazwisko, płeć, datę urodzenia, serię i numer paszportu lub innego dokumentu potwierdzającego tożsamość oraz kraj pochodzenia (art. 28).
Zgodnie zaś z art. 43 ust. 1 pkt 2 lit. a) ustawy o SIO, dane identyfikacyjne i dane dziedzinowe do zbioru danych nauczyciela w związku z awansem zawodowym przekazuje organ, który nadał nauczycielowi stopień awansu zawodowego, a w przypadku nauczyciela zatrudnionego w publicznej szkole i placówce oświatowej prowadzonej przez osobę prawną inną niż jednostka samorządu terytorialnego lub osobę fizyczną oraz w niepublicznej szkole i placówce oświatowej – szkoła lub placówka oświatowa, w której nauczyciel jest zatrudniony. Z kolei dane identyfikacyjne i dane dziedzinowe do zbioru danych nauczyciela przekazują pomioty wymienione w art. 43 ust. 1, m.in. szkoły i placówki oświatowe – w związku ze stosunkiem pracy.
W związku z powyższym o ile z przepisów ustawy o systemie informacji oświatowej wynika obowiązek przetwarzania numeru PESEL nauczyciela w systemie SIO, to jednak nie jest on wymagany przy składaniu wniosku o podjęcie postępowania egzaminacyjnego lub postępowania kwalifikacyjnego na podstawie art. 9b ust. 2a ustawy Karta Nauczyciela. Niemniej numer PESEL takiego nauczyciela już znajduje się w bazie SIO.
Reasumując, stwierdzić należy, że organ prowadzący szkołę nie ma podstawy prawnej do żądania ujawnienia numeru PESEL przez nauczyciela we wniosku o podjęcie postępowania egzaminacyjnego lub postępowania kwalifikacyjnego.

SZKOLENIA Z ZAKRESU RODO W ZWIĄZKU Z PRZEJŚCIEM PERSONELU W GRUPIE PRZEDSIĘBIORSTW

Oceniając potrzebę i zakres przeprowadzenia szkoleń z zakresu ochrony danych osobowych dla osób zmieniających pracodawcę w tej samej grupie przedsiębiorstw, należy brać pod uwagę m.in. różnice w procesach przetwarzania danych osobowych na poszczególnych stanowiskach pracy oraz specyfikę działania konkretnych podmiotów.

W związku z planem przejścia części personelu od jednego pracodawcy (na podstawie art. 231 Kodeksu pracy) do drugiego w tej samej grupie przedsiębiorstw (unia własnościowa), UODO został zapytany, jak wygląda kwestia przeszkolenia tych osób z perspektywy RODO. Czy konieczne jest ponowne ich przeszkolenie? Czy można uznać szkolenie odbyte u poprzedniego administratora jako aktualne u obecnego administratora?
W odpowiedzi organ nadzorczy wskazał, że RODO cechuje się podejściem opartym na zasadzie rozliczalności (o której mowa w art. 5 ust. 2) i ryzyku (o którym mowa zwłaszcza w art. 24 określającym obowiązki administratora i art. 39 ust. 2 odnoszącym się do zadań IOD. Zgodnie z tym podejściem, przyjmując określone rozwiązania, należy uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyka związane z operacjami przetwarzania. Dlatego RODO zazwyczaj nie wskazuje konkretnych rozwiązań, pozostawiając sporą swobodę wyboru administratorowi, a w zakresie wykonywania swoich zadań również inspektorowi ochrony danych, którzy powinni oceniać ryzyko związane z przetwarzaniem danych i dostosować swoje działania do poziomu tego ryzyka. Zatem działania podejmowane zarówno przez administratora, jak i przez inspektora ochrony danych powinny uwzględniać m.in. specyfikę podmiotu, w którym dane osobowe są przetwarzane.
Odnosząc te ogólne zalecenia do kwestii przedstawionej w pytaniu, organ nadzorczy wskazał, że szkolenia z ochrony danych osobowych powinny obejmować wskazówki dotyczące postępowania pracowników na określonych stanowiskach pracy, w określonej strukturze czy warunkach organizacyjnych. Dlatego oceniając potrzebę i zakres przeprowadzenia takich szkoleń, należy brać pod uwagę różnice występujące między konkretnymi stanowiskami pracy i procesami przetwarzania danych, do których dochodzi w związku z wykonywanymi obowiązkami służbowymi, a także różnice w działaniu konkretnych podmiotów i zachodzące zmiany organizacyjne.
Jednocześnie należy pamiętać, że to administrator (pracodawca) odpowiada za bezpieczeństwo danych osobowych, które przetwarza, a także za wszystkie osoby przetwarzające te dane w jego imieniu. Dlatego to w jego interesie leży, aby wszystkie te osoby miały odpowiednią wiedzę i kwalifikacje w zakresie ochrony danych osobowych.
Warto też dodać, że do kwestii prawidłowego prowadzenia szkoleń pracowników w zakresie ochrony danych osobowych i wskazywania ich jako stosowanego środka bezpieczeństwa danych organ nadzorczy odnosił się m.in. w decyzji nakładającej administracyjną karę pieniężną na jednego z burmistrzów.

3 WYBRANE DECYZJE UODO

PRACOWNIK NA L4, A POTRZEBNY JEST Z NIM KONTAKT TELEFONICZNY. I CO NA TO RODO?

To, jakie dane osobowe i na jakich zasadach może przetwarzać administrator wynika z ogólnego rozporządzenia o ochronie danych lub przepisów szczególnych. Utrzymanie dobrych relacji z kontrahentem to nie jest powód, który usprawiedliwia administratora, jeśli ten posłuży się danymi, do których nie jest uprawniony. Tym bardziej gdy w grę wchodzi przekazywanie informacji o powodach nieobecności tego pracownika związanych ze stanem zdrowia.

W jednej ze spraw zainicjowanych skargą osoby fizycznej Prezes UODO odniósł się do postępowania pewnego pracodawcy, którego upomniał w dwóch kwestiach. Po pierwsze, za naruszenie art. 6 ust. 1 RODO polegające na przetwarzaniu danych osobowych pracownika w zakresie prywatnego numeru telefonu bez podstawy prawnej. Po drugie, za naruszenie art. 9 ust. 1 RODO polegające na udostępnieniu na rzecz osób nieuprawnionych danych osobowych tego pracownika w zakresie danych dotyczących zdrowia, tj. udostępnieniu informacji o fakcie przebywania przez ww. na zwolnieniu lekarskim.

Posługiwanie się numerem telefonu prywatnego możliwe tylko za zgodą jego posiadacza

Pierwszym z rozpatrywanych w toku sprawy działań spółki było przetwarzanie przez nią danych osobowych skarżącej w postaci prywatnego numeru telefonu bez podstawy prawnej. RODO określa obowiązki administratora, do których należy przetwarzanie danych osobowych z zachowaniem przesłanek określonych w tym rozporządzeniu. Przepisem uprawniającym administratorów do przetwarzania danych osób fizycznych jest art. 6 ust. 1 RODO, zgodnie z którym, przetwarzanie jest dopuszczalne tylko wtedy, gdy spełniona jest jedna z przesłanek wskazanych w tym przepisie. Katalog przesłanek wymienionych w art. 6 ust. 1 RODO jest zamknięty. Każda z przesłanek legalizujących proces przetwarzania danych osobowych ma charakter autonomiczny i niezależny. Oznacza to, że ww. przepis legalizuje przetwarzanie danych, gdy spełniona jest co najmniej jedna z enumeratywnie wskazanych w nim przesłanek. Materiał dowodowy nie wykazał, żeby osoba skarżąca w jakikolwiek sposób dobrowolnie udostępniła swój prywatny numer telefonu, zarówno prezesowi zarządu spółki, jak i samej spółce do celów służbowych. Spółka w swoich wyjaśnieniach wskazała, że korespondencja mogła omyłkowo i niecelowo być prowadzona również z kontem użytkownika przypisanym do numeru prywatnego. Równocześnie spółka posiadała inne możliwości uzyskania kontaktu z osobą skarżącą, dysponując służbowym adresem e-mail oraz służbowym numerem telefonu komórkowego.
Po zbadaniu tego wątku w sprawie Prezes UODO stwierdził, że spółka nie legitymowała się żadną z przesłanek art. 6 ust. 1 RODO, kontaktując się z osobą skarżącą w celach służbowych na prywatny numer telefonu tej osoby.

3 WYBRANE DECYZJE UODO

Dane o stanie zdrowia. Ich przetwarzanie podlega szczególnym rygorom

Drugim z rozpatrywanych w toku sprawy działań spółki było udostępnienie danych osoby skarżącej w zakresie informacji o przebywaniu na zwolnieniu lekarskim oraz treści tego zwolnienia osobom trzecim. RODO określa obowiązki administratora, do których należy przetwarzanie danych osobowych z zachowaniem przesłanek określonych w tym rozporządzeniu. Przepisem uprawniającym administratora do przetwarzania szczególnych kategorii danych osobowych jest art. 9 ust. 1 oraz 2 RODO. Zgodnie z art. 9 ust. 1 RODO zabrania się przetwarzania m.in. danych osobowych dotyczących zdrowia osoby fizycznej. Zgodnie z art. 9 ust. 2 RODO, art. 9 ust. 1 RODO nie ma zastosowania, gdy spełniona jest jedna z przesłanek wskazanych w tym przepisie. Katalog przesłanek wymienionych w art. 9 ust. 2 RODO jest zamknięty. Każda z przesłanek legalizujących proces przetwarzania danych osobowych ma charakter autonomiczny i niezależny. Oznacza to, że ww. przepis legalizuje przetwarzanie danych, gdy spełniona jest co najmniej jedna z enumeratywnie wskazanych w nim przesłanek.

Informacje o przebywaniu przez daną osobę na zwolnieniu lekarskim oraz przybliżona treść zwolnienia stanowią dane dotyczące zdrowia, a więc jedną ze szczególnych kategorii danych enumeratywnie wymienionych w art. 9 ust. 1 RODO. Zgodnie bowiem z motywem 35 RODO do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą.

Do danych takich należą m.in. wszelkie informacje, na przykład o chorobie, ryzyku choroby, historii medycznej, stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia. Ponadto art. 4 pkt 15 RODO definiuje dane dotyczące zdrowia jako dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia. Informacja o przebywaniu przez osobę skarżącą na zwolnieniu lekarskim jest daną dotyczącą zdrowia, ponieważ ujawnia informację o stanie zdrowia tej osoby oraz o korzystaniu przez nią z usług opieki zdrowotnej, jako że sam fakt otrzymania zwolnienia lekarskiego oznacza, że osoba ta z takiej usługi skorzystała, jak również, że z uwagi na stan zdrowia nie powinna ona wykonywać pracy na zajmowanym stanowisku.

W omawianej sprawie spółka uzasadniała udostępnienie tych danych osobom trzecim koniecznością wytłumaczenia kontrahentom spółki powodów utrudnionego kontaktu z tym podmiotem, jak również koniecznością reorganizacji obowiązków pozostałych pracowników w świetle nieobecności osoby skarżącej w pracy.

Zdaniem organu nadzorczego, powyższe powody nie stanowią żadnej z przesłanek z art. 9 ust. 2 RODO legalizujących proces przetwarzania szczególnych kategorii danych osobowych, jakim w zakresie niniejszego postępowania jest ich udostępnienie osobom trzecim.

4 NARUSZENIA I KONTROLE

SUKCESYWNE PRZEKAZYWANIE ORGANOWI NADZORCZEMU INFORMACJI O NARUSZENIU

Co do zasady RODO nakłada na administratorów obowiązek zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych w terminie 72 godzin od jego stwierdzenia. Dotychczasowa praktyka pokazuje jednak, że w niektórych sytuacjach administratorzy mogą potrzebować więcej czasu na zgromadzenie informacji niezbędnych do dokonania prawidłowego zgłoszenia. Co mogą zrobić, aby w takim przypadku uniknąć opóźnienia i nie narazić się na administracyjną karę pieniężną?

Projektując kwestie związane z obowiązkiem notyfikacyjnym, unijny prawodawca uwzględnił sytuacje, w których administratorzy nie będą dysponować wszystkimi wymaganymi informacjami dotyczącymi naruszenia w ciągu 72 godzin od momentu jego stwierdzenia. W związku z tym, stosownie do art. 33 ust. 4 RODO, mogą oni przekazywać informacje sukcesywnie, dokonując w odpowiednim terminie zgłoszenia wstępnego, stopniowo uzupełnianego za pośrednictwem kolejnych zgłoszeń w miarę pozyskiwania brakujących informacji o naruszeniu.

Kiedy administrator może dokonać niepełnego zgłoszenia?

W Wytycznych 9/2022 w sprawie zgłaszania naruszeń ochrony danych osobowych zgodnie z RODO (Guidelines 9/2022 on personal data breach notification under GDPR – version 2.0) EROD wskazuje, iż przytoczony przepis odnosi się do sytuacji, w których administratorzy nie mają możliwości dokonania szczegółowych i rzetelnych ustaleń dotyczących naruszenia oraz związanych z nim konsekwencji w jego początkowej fazie. Dotyczy to w szczególności bardziej złożonych incydentów (np. z zakresu cyberbezpieczeństwa), w przypadku których – w celu kompletnego określenia charakteru naruszenia, zakresu, w jakim dane osobowe zostały naruszone czy liczby osób, których te dotyczą – konieczne mogą okazać się m.in. specjalistyczne badania z zakresu informatyki śledczej i analizy powłamaniowej. W rezultacie administratorzy mają możliwość przekazania organowi nadzorczemu uzyskanych w ten sposób informacji poprzez zgłoszenie uzupełniające w terminie późniejszym, tj. po upływie 72 godzin.

4 NARUSZENIA I KONTROLE

Zgłoszenia kompletne/jednorazowe, wstępne i uzupełniające/zmieniające

Podkreślenia wymaga, że w takiej sytuacji administratorzy wciąż będą zobowiązani do dokonania terminowego zgłoszenia wstępnego, w treści którego powinni określić rodzaj dokonywanego zgłoszenia (kompletne/jednorazowe, wstępne lub uzupełniające/zmieniające), wybierając odpowiednią rubrykę w pierwszej sekcji formularza dostępnego na stronie internetowej Urzędu Ochrony Danych Osobowych (www.uodo.gov.pl), a także wskazać przyczyny jego ewentualnego opóźnienia oraz przybliżoną datę uzupełnienia. EROD zaleca, aby administrator powiadamiając po raz pierwszy organ nadzorczy o naruszeniu jasno zaznaczył, iż nie posiada jeszcze wszystkich wymaganych informacji, w związku z czym przekaże brakujące szczegóły w późniejszym terminie. Nie uniemożliwia to administratorowi przekazania organowi nadzorczemu informacji również na innym etapie, o ile dowie się o dodatkowych znaczących faktach dotyczących naruszenia (także wtedy, gdy zdobędzie dowody wskazujące na to, że do naruszenia nie doszło).

Obowiązki administratora w obszarze identyfikacji naruszeń

Niezależnie od powyższego należy pamiętać, iż po uzyskaniu pierwszych informacji o potencjalnym incydencie administrator powinien bezzwłocznie przeprowadzić wewnętrzne postępowanie wyjaśniające w celu ustalenia wszelkich istotnych okoliczności zdarzenia. Oczekuje się, że ocena wstępna, pozwalająca z wystarczającą dozą pewności uznać, że doszło do naruszenia ochrony danych osobowych, zostanie przeprowadzona możliwie jak najszybciej. Do obowiązków administratora należy bowiem wdrożenie odpowiednich środków technicznych i organizacyjnych umożliwiających jak najszybsze stwierdzenie, czy rzeczywiście doszło do naruszenia oraz terminowe zawiadomienie o nim organu nadzorczego, a także – w stosownych przypadkach – osób, których dane dotyczą.

5 NOWE TECHNOLOGIE

„DARK PATTERNS" – CZYLI ZWODNICZE INTERFEJSY W SKETORRZE CYFROWYM

W 2023 roku Komisja Europejska i krajowe organy ds. ochrony konsumentów opublikowały wyniki akcji kontrolnej stron internetowych, przeprowadzonej pod kątem stosowania praktyk manipulacyjnych, które wymuszają niechciane przez klientów działania. Okazało się, że prawie 40 proc. z 399 badanych sklepów internetowych należących do sprzedawców detalicznych stosuje tego typu nieuczciwe praktyki, w celu wykorzystania podatności konsumentów.

Zwodnicze interfejsy (dark patterns), bo o nich mowa, to szkodliwe praktyki, które mogą naruszać nie tylko przepisy RODO i przepisy o ochronie konsumentów, ale również aktu o usługach cyfrowych (DSA), który w pełni będzie stosowany od 17 lutego 2024 r. Czym dokładnie są i jak się przed nimi chronić?
Dark patterns mogą przybierać bardzo różne formy. Stosowane są m.in. w banerach dotyczących przetwarzania danych osobowych. Przykładem może być np. eksponowanie przycisku „Akceptuj" na banerze dotyczącym zgody na pliki cookie, często połączonym z niejasno sformułowanym komunikatem, podczas gdy przycisk akceptujący wyłącznie niezbędne pliki cookies pozostaje znacznie mniej widoczny. Innym przykładem jest wizualne zasłanianie ważnych informacji, np. o możliwości anulowania subskrypcji, a eksponowanie opcji korzystnej dla firmy, czy też licznik odliczający czas do zakończenia akcji promocyjnej z sugestią natychmiastowego zakupu.

> Jak wskazano w motywie 67 przywołanego aktu o usługach cyfrowych: „Zwodnicze interfejsy na interfejsach internetowych platform internetowych to praktyki, które w istotny sposób zniekształcają lub ograniczają, celowo lub w praktyce, zdolność odbiorców usługi do dokonywania niezależnych i świadomych wyborów lub podejmowania takich decyzji. Praktyki te mogą być wykorzystywane w celu nakłonienia odbiorców usługi do niepożądanego zachowania lub do podejmowania niepożądanych decyzji, które mają dla nich negatywne skutki(...)".
>
> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)

W przyjętym akcie o usługach cyfrowych wprowadzono zakaz wykorzystywania zwodniczych interfejsów (dark patterns) do wprowadzania w błąd lub nakłaniania odbiorców usługi do określonego działania (często w sposób nieświadomy). Przepisy dotyczące zwodniczych interfejsów należy interpretować w taki sposób, aby obejmowały zakazane praktyki wchodzące w zakres stosowania niniejszego rozporządzenia w zakresie, w jakim praktyki te nie są już objęte zakresem stosowania, chociażby przez RODO.
Z kolei w lutym 2023 r. Europejska Rada Ochrony Danych przyjęła Wytyczne 3/2022 zawierające praktyczne zalecenia i wskazówki dla dostawców mediów społecznościowych dotyczące projektowania zwodniczych wzorców projektowych, które naruszają wymogi RODO. W celu lepszego oddania różnorodności stosowanych praktyk, EROD w swoich wytycznych zastąpiła pojęcie „zwodnicze interfejsy" (dark patterns) szerszym pojęciem „zwodnicze wzorce projektowe" (deceptive design patterns).

5 NOWE TECHNOLOGIE

I choć wytyczne odnoszą się do platform społecznościowych, można odnieść je do całego sektora cyfrowego, w którym stosowane są tego typu nieuczciwe praktyki. Wytyczne mają na celu przypomnienie obowiązków wynikających z RODO, ze szczególnym uwzględnieniem zasad zgodności z prawem, rzetelności, przejrzystości, celowości i minimalizacji danych podczas projektowania interfejsów użytkownika.

Zgodnie z wytycznymi 3/2022: „Zwodnicze wzorce projektowe to interfejsy i ścieżki użytkownika realizowane na platformach mediów społecznościowych, których celem jest wpłynięcie na użytkowników w celu dokonania niezamierzonych, odpowiednio niechętne i/lub potencjalnie szkodliwych decyzji, często w kierunku opcji sprzecznej z najlepszym interesem użytkowników i sprzyjającej interesom platform mediów społecznościowych w odniesieniu do ich danych osobowych(...)".

Wytyczne 3/2022 w sprawie zwodniczych wzorców projektowych w interfejsach platform społecznościowych

Stosowanie zwodniczych wzorców projektowych może stanowić zagrożenie nie tylko z punktu widzenia dokonywania nieprzemyślanych i potencjalnie szkodliwych dla użytkownika decyzji, ale również – co jest jeszcze bardziej istotne – dla ochrony danych osobowych. Ważne jest, aby projektanci interfejsów mieli na uwadze zasady wynikające z RODO. Przede wszystkim powinni upewnić się, że prawidłowo wdrażają zasady określone w art. 5 RODO, w tym zasadę rozliczalności, minimalizacji danych i ograniczenia celu.

Dark patterns mogą skłaniać użytkowników do nieświadomego wyrażania zgody na zbieranie lub udostępnianie swoich danych osobowych. Warunki wyrażenia zgody określone zostały w art. 7 RODO. Zgoda powinna być wyrażona poprzez „wyraźne działanie potwierdzające", dlatego domyślnie zaznaczone pole nie stanowi wyraźnej i świadomej zgody użytkownika. Niedopuszczalne jest używanie interfejsu nakierowanego na wymuszenie zgody poprzez jego nietransparentną formę, niepozostawiającą użytkownikowi możliwości na dobrowolne, konkretne, świadome i jednoznaczne okazanie woli. Ponadto administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie.

Istotna z punktu widzenia zwodniczych interfejsów jest również zasada przejrzystości szczegółowo opisana w art. 12 ust. 1 RODO. Tym bardziej, że tego typu praktyki zmierzają do zaciemnienia przekazu i wprowadzenia użytkownika w błąd, manipulując nim w taki sposób, aby podjął niezamierzoną i często potencjalnie szkodliwą decyzję. Zgodnie z art. 12 RODO wymagane jest, aby wszelka komunikacja i udzielanie informacji osobom, których dane dotyczą odbywały się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie. Należy również pamiętać, że osoby, których dane dotyczą mają również prawo sprzeciwu wobec przetwarzania ich danych osobowych zgodnie z art. 21 RODO.

Istotną rolę odgrywają także wymogi dotyczące ochrony danych w fazie projektowania i domyślnej ochrony danych zgodnie z art. 25 RODO. EROD w Wytycznych 3/2022 podkreśla, że zastosowanie tych zasad przed uruchomieniem projektu interfejsu z pewnością umożliwiłoby dostawcom mediów społecznościowych uniknąć stosowania nieuczciwych praktyk.

5 NOWE TECHNOLOGIE

Niestety, stosowanie zwodniczych interfejsów w sektorze cyfrowym może prowadzić nie tylko do naruszenia przepisów dotyczących ochrony konsumentów, ale również o ochronie danych osobowych, dlatego kwestia ich wykorzystania jest brana pod uwagę przez unijne i krajowe organy zajmujące się ochroną danych i ochroną konsumentów. Istotne jest bowiem, aby projektowanie interfejsów odbywało się zgodnie z obowiązującymi wymogami prawnymi.

Niestety stosowanie zwodniczych interfejsów w sektorze cyfrowym może prowadzić nie tylko do naruszenia przepisów dotyczących ochrony konsumentów, ale również o ochronie danych osobowych, dlatego kwestia ich wykorzystania jest brana pod uwagę przez unijne i krajowe organy zajmujące się ochroną danych i ochroną konsumentów. Istotne jest bowiem, aby projektowanie interfejsów odbywało się zgodnie z obowiązującymi wymogami prawnymi.

7 SPRAWY MIĘDZYNARODOWE

POSTĘPOWANIE TRANSGRANICZNE CZEKAJĄ ZMIANY

Komisja Europejska zaproponowała nowe przepisy mające usprawnić współpracę między organami ochrony danych podczas egzekwowania ogólnego rozporządzenia o ochronie danych (RODO) w sprawach transgranicznych.

W nowym rozporządzeniu zostaną ustanowione konkretne przepisy proceduralne dla organów stosujących RODO w sprawach, które dotyczą obywateli z różnych państw członkowskich. Rozporządzenie zobowiąże na przykład wiodący organ ochrony danych do przesyłania streszczeń kluczowych kwestii do jego odpowiednika w innym państwie. W streszczeniach będą uwzględnione najważniejsze elementy dochodzenia oraz opinia organu na temat danej sprawy na wczesnym etapie postępowania. Pozwoli to ograniczyć liczbę nieporozumień i ułatwi szybkie osiąganie konsensusu.
Nowe przepisy mają za zadanie zapewnić odpowiednie zaangażowanie obywateli w proces i doprecyzują, jakie dokumenty należy przedłożyć na etapie składania skargi. W odniesieniu do organów ochrony danych nowe przepisy usprawnią współpracę i zwiększą skuteczność egzekwowania przepisów.

INDIE PRZYJĘŁY USTAWE DOTYCZĄCĄ OCHRONY CYFROWYCH DANYCH OSOBOWYCH

**Po sześciu latach starań, Indie przyjęły ustawę o ochronie danych osobowych przetwarzanych.
To skutek jednego z wyroków Sądu Najwyższego Indii, który uznał prywatność za prawo podstawowe.**

Nowo przyjęty akt prawa gwarantuje prawo do sprostowania i usunięcia danych osobowych. Wśród wyjątków od stosowania ustawy znajduje się przypadek publicznego udostępnienia przez podmiot danych jego danych osobowych. Ustawodawca podaje przykład takiej sytuacji – osoba fizyczna, opisując na platformie internetowej swoje poglądy, publicznie udostępnia swoje dane osobowe w mediach społecznościowych. W takiej sytuacji nowo przyjęta ustawa nie będzie miała zastosowania.
Co istotne, ustawa ma zastosowanie także do przetwarzania cyfrowych danych osobowych poza Indiami, „jeśli takie przetwarzanie jest związane z jakąkolwiek działalnością związaną z oferowaniem towarów lub usług podmiotom danych na terytorium Indii".
Ponadto ustawa tworzy Radę Ochrony Danych Indii, która zostanie ustanowiona przez rząd z pewnymi gwarancjami niezależności, a jej członkowie będą mianowani przez rząd tylko na dwuletnią kadencję

Źródło: komunikat

7 SPRAWY MIĘDZYNARODOWE

SZWECJA: PIERWSZA WYSOKA ADMINISTRACYJNA KARA PIENIĘŻNA ZA UŻYWANIE GOOGLE ANALYTICS

Szwedzki organ ochrony danych przeprowadził postępowanie wobec czterech przedsiębiorstw wykorzystujących Google Analytics do statystyk internetowych. Organ nałożył kary administracyjne na dwa z nich. Jeden podmiot niedawno zaprzestał korzystania z narzędzia statystycznego z własnej inicjatywy, podczas gdy pozostałym trzem zaprzestanie korzystania z ww. narzędzia nakazał szwedzki organ ochrony danych.

Szwedzki organ ochrony danych skontrolował sposób, w jaki cztery przedsiębiorstwa (CDON, Coop, Dagens Industri i Tele2) przekazują dane osobowe do USA za pośrednictwem Google Analytics, który jest narzędziem do pomiaru i analizy ruchu na stronach internetowych. Postępowanie opierało się na skargach organizacji None of Your Business (NOYB) złożonych w świetle orzeczenia Schrems II wydanego przez TSUE. Wszystkie cztery przedsiębiorstwa oparły swoje decyzje dotyczące przekazywania danych osobowych za pośrednictwem Google Analytics na standardowych klauzulach umownych. Z inspekcji przeprowadzonej przez szwedzki organ ochrony danych wynika, że żadne z dodatkowych technicznych środków bezpieczeństwa nie były wystarczające. Organ nadzorczy nałożył administracyjną karę pieniężną w wysokości 12 milionów koron szwedzkich na Tele2 i 300 000 koron szwedzkich na CDON. Tele2 niedawno zaprzestało korzystania z Google Analytics z własnej inicjatywy. Szwedzki organ ochrony danych nakazał pozostałym trzem przedsiębiorstwom zaprzestanie korzystania z tego narzędzia.
Źródło: komunikat

FRANCJA: KARA PIENIĘŻNA ZA STOSOWANIE SPERSONALIZOWANYCH REKLAM BEZ ZGODY

Francuski organ ochrony danych (CNIL) ukarał w czerwcu 2023 roku CRITEO, spółkę specjalizującą się w reklamie internetowej, administracyjną karą pieniężną w wysokości 40 mln euro, w szczególności za brak weryfikacji, czy osoby, których dane przetwarzała, wyraziły na to zgodę.

W następstwie skarg złożonych przez organizacje Privacy International i None of Your Business, CNIL przeprowadził kilka postępowań w sprawie CRITEO.
W ich wyniku organ nadzorczy potwierdził istnienie kilku naruszeń, obejmujących w szczególności brak dowodów uzyskania zgody od osób fizycznych na przetwarzanie ich danych, realizacji obowiązków informacyjnych i przestrzegania zasady przejrzystości, a także poszanowania praw osób, których dane dotyczą, takich jak prawo dostępu do danych, prawo wycofania zgody i usunięcia danych. Ponadto CNIL stwierdził niedopełnienie obowiązku zawarcia porozumienia między współadministratorami (art. 26 RODO).
Źródło: decyzja organu nadzorczego

SKUETCZNA OCHRONA DANYCH OSOBOWYCH. CZY WARTO MÓWIĆ O TYM DZIECIOM?

Podniesienie kompetencji pedagogów i nauczycieli oraz edukowanie dzieci i młodzieży, jak mają chronić dane osobowe zarówno w realnym, jak i w cyfrowym świecie, to główne cele ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa". Właśnie trwa nabór.

Od 1 września do 30 listopada br. placówki oświatowe mogą zgłaszać swoje uczestnictwo w XIV edycji tego programu. W tym roku szkolnym tematem przewodnim programu będzie ochrona danych osobowych w mediach społecznościowych i nie tylko.
Program poprzez zabawę i naukę zachęca nauczycieli i uczniów do bliższego poznania podstawowych zasad ochrony danych osobowych, aby po pierwsze wiedzieli, jakie prawa gwarantuje im RODO, a po drugie korzystali z nich, co jest istotne w dobie gwałtowanego rozwoju nowych technologii.

Systemowa edukacja w całej Polsce

Program „Twoje dane – Twoja sprawa" jest realizowany nieprzerwanie od 2009 roku pod honorowym patronatem Ministra Edukacji Narodowej i Rzecznika Praw Dziecka.
Program „Twoje dane – Twoja sprawa" – skierowany do szkół podstawowych, ponadpodstawowych oraz ośrodków doskonalenia nauczycieli – jest systemowym projektem edukacyjnym Urzędu Ochrony Danych Osobowych realizowanym na skalę ogólnopolską.

Dwa etapy realizacji programu

Program jest realizowany w dwóch etapach:

- najpierw wiedzę z zakresu ochrony danych osobowych i prawa do prywatności poszerzają nauczyciele, którzy m.in. biorą udział w dwudniowej konferencji szkoleniowo-informacyjnej, podczas której UODO przekazuje im pakiet materiałów edukacyjnych, w skład którego wchodzą: broszury informacyjne dotyczące zasad przetwarzania danych osobowych, scenariusze lekcji, prezentacje multimedialne i inne pomoce dydaktyczne ułatwiające realizację Programu. Materiały te i informacje są obowiązkowo przekazywane również radom pedagogicznym,
- w kolejnym etapie nauczyciele wiedzę zdobytą podczas szkolenia upowszechniają wśród uczniów, zarówno podczas lekcji z różnych przedmiotów, jak i podejmując się wdrażania innych niestandardowych działań.

Szczegółowe informacje o programie są dostępne na stronie internetowej UODO w zakładce „Co robimy'

8 WSPÓŁPRACA Z UODO

JAK KORZYSTAMY Z INTERNETU W DOBIE KOMUNIKACJI ELEKTRONICZNEJ?

Usługi komunikacji elektronicznej weszły do codziennego życia, zarówno w przestrzeni prywatnej, jak i w stosunkach gospodarczych. Rozwój narzędzi cyfrowych zmienił i nadal bardzo szybko zmienia oblicze świata, w którym żyjemy. XXI wiek to doba społeczeństwa informacyjnego i nowych technologii informacyjno-komunikacyjnych. Wpływają one na gospodarkę, przyśpieszając jej rozwój oraz przeobrażają naszą rzeczywistość.

Wyzwaniem czasów cyfrowych i społeczeństwa informacyjnego jest przede wszystkim skuteczna ochrona obywatela, klienta jako uczestnika obrotu cyfrowego.
Jeśli mówimy o osobie fizycznej, kluczowe znaczenie odgrywa w cyberświecie:
bezpieczeństwo danych osobowych i ich ochrona, świadomość prawa do prywatności, świadomość zagrożeń jakie mogą nas spotkać w sieci.
Mówiąc o możliwościach i korzyściach korzystania z usług komunikacji elektronicznej trzeba zadać sobie pytanie, jak zadbać o własne bezpieczeństwo i bezpieczeństwo w sieci swoich klientów. Kluczowe znaczenie ma to, czy i jak możemy stworzyć bezpieczne warunki dla naszych danych w świecie cyfrowym. Czy możemy uchronić się przez cyberatakami?
Rokrocznie przeprowadzane są przez Urząd Komunikacji Elektronicznej badania i analizy prezentujące sposób, w jaki korzystamy z technologii informacyjno-komunikacyjnych.
W 2022 roku Urząd Komunikacji Elektronicznej przeprowadził badanie klientów indywidualnych, w tym poddając badaniu także zachowania Polaków w obszarze bezpieczeństwa w sieci.
Z badania wynika, że coraz mocniej troszczymy się o swoje bezpieczeństwo, korzystając z usług komunikacji elektronicznej. Większość z badanych deklaruje, że korzysta z programów antywirusowych lub antyspyware (71%), aktualnego oprogramowania (73,3%), a ponad połowa z nich zabezpiecza także swoje urządzenie mobilne, korzystając z programów antywirusowych i antyspyware (54,3%). Ponad 2/3 respondentów zadeklarowało, że potrafi sprawdzić, czy korzysta z bezpiecznego połączenia z Internetem.
Bardzo ważne jest budowanie świadomości odnośnie do kwestii prywatności w sieci i ochrony danych osobowych. 81% badanych zadeklarowało, że prywatność w sieci ma dla nich duże znaczenie. Natomiast blisko co dziesiąta osoba badana wskazywała, że ten obszar nie stanowi dla niej wartości (podobna liczba osób badanych nie wyraziła zdania na ten temat). Ważne jest też to, że korzystamy z rozwiązań zwiększających poziom prywatności w sieci (37% badanych). Wśród popularnych narzędzi, respondenci wskazywali między innymi:

- programy antywirusowe,
- bezpieczne przeglądarki,
- VPN,
- szyfrowanie wiadomości i połączeń.

8 WSPÓŁPRACA Z UODO

Bardzo ważnym pytaniem, które należy postawić jest, jak postrzegamy udostępnianie informacji o sobie w Internecie i komu je udostępniamy? Aż 83,5% respondentów ma świadomość udostępniania swoich danych osobowych w sieci. Z drugiej strony, aż 16,1% uczestników badania nie zdaje sobie z tego sprawy. W większości (blisko 60%) ankietowanych wskazywało, że udostępnia dane osobowe w Internecie podmiotom publicznym i instytucjom finansowym, blisko połowa wskazała, że przedsiębiorstwom (np. sklepom internetowym), a co ponad czwarty badany portalom społecznościowym.

Problemem nadal pozostaje niechęć klientów do zapoznawania się z dokumentacją umowną związaną z korzystaniem z usług internetowych (poczta, komunikatory publiczne sieci Wi-Fi) przed ich akceptacją. Ponad połowa badanych zadeklarowała, że robiła to tylko czasami. To wpływa na poziom świadomości praw i obowiązków użytkowników, warunków świadczenia usługi, a co za tym idzie bezpieczeństwo klienta w sieci.

Z całą pewnością te dane pokazują pozytywne obszary dotyczące wzmacniania świadomości w sieci i bezpieczeństwa danych, ale także wskazują, jak duże pole do działania i wyzwania stoją przed organami państwa i rynkiem, by nadal, konsekwentnie wzmacniać świadomość i bezpieczeństwo użytkowników w Internecie. Kształtowanie właściwych postaw i zasilanie w wiedzę konsumentów jest kluczowym obecnie zadaniem, którego realizacja realnie może wpłynąć na poziom bezpieczeństwa obywatela cyfrowego.

Corocznie Urząd Komunikacji Elektronicznej prowadzi także badanie konsumenckie dzieci i rodziców, które daje wiedzę na temat tego, jak wygląda wzór korzystania z narzędzi komunikacji elektronicznej przez najmłodszych. Dzieci zwykle zaczynają korzystać z telefonu komórkowego w wieku 7–10 lat (7–8 lat – 38,3%, 9–10 lat – 41,4%). Niemal każde dziecko ma telefon typu smartfon (96,9%). Większość dzieci korzysta z Internetu w różnych obszarach, poza edukacją online (91,3%). Najczęściej w świat Internetu dzieci wkraczają w wieku 7–8 lat (38,8%), ale aż 23,1% dzieci w trakcie badania wskazywało, że zaczęło korzystać z sieci mając 5–6 lat. Dzieci najwięcej czasu spędzają w Internecie oglądając filmy na YouTube, grając w gry, przeglądając strony internetowe oraz korzystając z komunikatorów i portali społecznościowych.

Dostęp do Internetu to swobodny dostęp do różnorodnych zasobów. Z tego względu niezwykle ważne jest edukowanie najmłodszych użytkowników usług komunikacji elektronicznej, co do bezpiecznego korzystania z usług cyfrowych, wartości danych osobowych, bezpieczeństwa tych danych i możliwych zagrożeń, zgodnie z powiedzeniem „Czego Jaś się nie nauczy, tego Jan nie będzie umiał".

8 WSPÓŁPRACA Z UODO

Internet to łatwość załatwiania spraw online czy możliwości: pracy i edukacji na odległość, korzystania z usług i wymiany towarów z całego świata, załatwiania spraw urzędowych. Jest atrakcyjnym narzędziem dla każdego. Urząd Komunikacji Elektronicznej promuje bezpieczne korzystanie z Internetu i zwraca szczególną uwagę na edukowanie w obszarze możliwych zagrożeń i metod ich eliminowania, zapobiegania im i właściwych postaw w cyberświecie.

Pozytywne jest to, że rośnie świadomość konsumentów, jeśli chodzi o kwestie prawa do prywatności, wartości danych osobowych i konieczności zapewnienia bezpieczeństwa danych. Jest jednak ciągle wiele do zrobienia, o czym mówią badania wskazane w niniejszym materiale.

Urząd Komunikacji Elektronicznej wspiera wszystkich użytkowników usług cyfrowych. Aktywnie prowadzone kampanie edukacyjne „Klikam z głową" czy „Ja online" wpisały się na stałe w krajobraz edukacji cyfrowej na terenie całego kraju. Skierowane są do wszystkich grup dzieci, młodzieży, dorosłych, seniorów, nauczycieli, edukatorów. O szczegółach akcji edukacyjnych Urzędu Komunikacji Elektronicznej można przeczytać na stronie Centrum Informacji Konsumenckiej.

Dorota Grudzień-Barbachowska, Dyrektor Departamentu Polityki Konsumenckiej, Urząd Komunikacji Elektronicznej

UKE

PRZYPISY

[1] **Badanie konsumenckie klientów indywidualnych przeprowadzone w 2022 roku - Urząd Komunikacji Elektronicznej**

[2] **Badanie konsumenckie dzieci i rodziców przeprowadzone w 2022 - Centrum Informacji Konsumenckiej**

8 WSPÓŁPRACA Z UODO

KLUCZOWE ASPEKTY PROGRAMÓW STUDIÓW Z ZAKRESU OCHRONY DANYCH OSOBOWYCH

Ochrona danych osobowych w dzisiejszym świecie pełnym informacji, odgrywa szczególną rolę. Programy studiów związane z tą tematyką oferują uczestnikom nie tylko szansę na zdobycie wszechstronnej wiedzy teoretycznej i praktycznej, ale także stanowią odpowiedź na rosnące zapotrzebowanie na specjalistów w tej dziedzinie.

Zapraszamy do rozmowy z prof. dr hab. Jerzym Pisulińskim, Dziekanem Wydziału Prawa i Administracji Uniwersytetu Jagiellońskiego w Krakowie. Rozmawiał Adam Sanocki, Dyrektor Departamentu Komunikacji Społecznej, Rzecznik Prasowy UODO.

Jakie są najważniejsze cele programów studiów dedykowanych dla inspektorów ochrony danych oferowanych na Waszej uczelni?

Najważniejszym celem naszych studiów, organizowanych pod patronatem UODO, jest zapewnienie wszechstronnej, praktycznej i teoretycznej wiedzy z zakresu prawa, technologii i zarządzania. Program jest zaprojektowany tak, aby IOD byli w stanie efektywnie zarządzać bezpieczeństwem informacji w różnorodnych organizacjach. Obejmuje on nie tylko aspekty prawne, ale przedstawia także kluczowe dla zrozumienia cyberzagrożeń zagadnienia techniczne. Oba te elementy są niezbędne dla właściwej analiza ryzyka i procesu zarządzania danymi, zgodnego z obowiązującymi przepisami. Naszym celem jest zarówno przekazanie bardzo wszechstronnej i przede wszystkim praktycznej wiedzy z zakresu obecnych uregulowań tyczących ochrony danych, jak i przygotowanie IOD do proaktywnego przewidywania kierunków zmian w zakresie ochrony danych, w tym także zapobieganiu naruszeniom, oraz do dzielenia się tą wiedzą z personelem.

W jaki sposób uczelnia dostosowuje programy edukacyjne w zakresie ochrony danych do dynamicznie zmieniającego się środowiska regulacyjnego czy biznesowego?

W reakcji na dynamicznie zmieniające się środowisko prawne i otoczenie regulacyjne, w obecnej edycji studiów całkowicie przebudowany został ich program.

8 WSPÓŁPRACA Z UODO

Zupełnie nowa odsłona programu obejmuje pogłębioną analizę obowiązujących uregulowań i wyzwań, przed jakimi stoją IOD, a także, co warto podkreślić, uwzględnia akty prawne, które znajdują się na ostatnich etapach procesu legislacyjnego (zwłaszcza na szczeblu unijnym). Pozwoli to słuchaczom na zrozumienie pełnego kontekstu dynamicznie zmieniającego się środowiska regulacyjnego i biznesowego. Mimo, że Rozporządzenie o Ochronie Danych Osobowych (RODO) obowiązuje od wielu lat, firmy wciąż mają problem z jego pełnym wdrożeniem, z uwagi na liczne zmiany w zakresie obowiązków, jakie RODO nakłada na administratorów. Z tego powodu w obecnej edycji studiów kompleksowo omówione zostaną m.in. zagadnienia związane z analizą ryzyka związanego z przetwarzaniem danych wraz praktycznymi wskazówkami jej przeprowadzania dla przetwarzających, wpływie orzecznictwa TSUE na system ochrony danych osobowych i wykładnię RODO czy niedoceniane często zalety związane z wdrożeniem kodeksów postępowania i certyfikacji.
Najlepszym przykładem jest tu pojawienie się wersji 3.5, a następnie 4 ChatGPT oraz ogrom problemów prawnych związanych z transgranicznym przetwarzaniem zbiorów danych w usługach chmurowych. To nagłe pojawienie się oprogramowania „działającej i ludzkiej" technologii generatywnej sztucznej inteligencji, oferowanej w zdecydowanej większości przez podmioty spoza EOG, wymusiło pilną potrzebę uchwalania przepisów na szczeblu unijnym i krajowym, tworząc jednocześnie stan, w którym z biznesowego punktu widzenia wykorzystywanie niewątpliwych zalet tego oprogramowania, równoważyć trzeba świadomością ryzyka, wynikającego z potencjalnego naruszenia obecnie obowiązujących regulacji.

Na co Państwa zdaniem należy zwrócić uwagę wybierając studia w zakresie ochrony danych osobowych? Jakie rady możecie dać Państwo osobom zainteresowanym studiami w tym zakresie?
Kluczowe są niewątpliwie kadra i program. Pomimo tego, że Uniwersytet Jagielloński to najstarsza uczelnia wyższa w Polsce, z najlepszym wydziałem prawa w kraju (wg. rankingów wydziałów prawa Dziennika Gazety Prawnej oraz Rzeczpospolitej z 2022 i 2023 roku), to rankingi, w których zdobywamy od lat czołowe miejsca, są tylko odzwierciedleniem ciągłego dążenia do doskonałości, nie tylko przez stałe aktualizowanie treści przekazywanych w ramach studiów, ale i wyszukiwaniu kadry, jaka ową wiedzę w przystępny sposób przekaże. Szczególnie dumni jesteśmy w tym kontekście ze współpracy, którą przed niemal 10 laty nawiązaliśmy z UODO w zakresie organizacji studiów. Liczne grono ekspertów z UODO, którzy wykładają na naszych studiach, jest gwarancją nie tylko najwyższego poziomu merytorycznego, ale najbardziej praktycznego charakteru oferowanych przez nas studiów. Mamy świadomość, że naszymi słuchaczami są praktycy, którzy oczekują konkretnej i praktycznej wiedzy, uświadomienia zagrożeń i sposobu zabezpieczenia się przed nimi. Współpraca z UODO umożliwia poznanie najczęstszych błędów, jakie popełniane są przez IOD, co w wymierny sposób przełoży się na uzyskanie szerokiej perspektywy wyzwań, z którymi mierzyć się będą jako IOD. Ponadto, pozwoli im uzyskać praktyczną wiedzę, jak owe wymagania spełnić. Przydatność studiów w pracy zawodowej, która jest wynikową powyższych aspektów, jest naszym kluczowym celem, bo to jest też to, czego szukają i oczekują nasi studenci.

8 WSPÓŁPRACA Z UODO

W jaki sposób uczelnia stara się przygotować inspektorów ochrony danych do radzenia sobie z coraz bardziej zaawansowanymi zagrożeniami związanymi z bezpieczeństwem danych, takimi jak cyberataki czy naruszenia danych?

W programie studiów przewidzieliśmy cały moduł, który od podstaw wyjaśni w przystępny sposób wszystkie zagadnienia techniczne związane z przetwarzaniem danych w systemach informatycznych, niezbędne w pracy IOD. Dla przykładu wskazać można, iż trudno tworzyć i wdrażać odpowiednią politykę ochrony danych uwzględniającą ich charakter oraz potencjalne zagrożenie, bez świadomości co sprawia, że hasła mogą zostać uznane w dzisiejszych czasach za bezpieczne. Świadomość, jak hasła są w dzisiejszych czasach łamane, jak wycieki w innych formach danych, mogą wpływać na bezpieczeństwo naszych danych, czym są luki 0-day i czemu za ich pomocą do naszego systemu można się włamać, pomimo podjęcia wszelkich środków zapobiegawczych, nabiera coraz większego znaczenia w kontekście dynamicznego rozwoju cyberprzestępczości.

Odrębne zajęcia poświęcimy także analizie wniosków o uprzednie konsultacje i ocenę skutków dla ochrony danych czy kwestii ich profilowania i przekazywania do państw trzecich. Zwłaszcza ten ostatni aspekt doskonale uwidacznia konieczność adaptacji i elastycznego reagowania na nowe wyzwania, jakie niosą za sobą zmieniające się technologie. Zmieniające się modele działania cyberprzestępców, wykorzystywanie multivector attacs, ekstrakcja danych połączona z równoległym atakiem ransomware i szantażowanie firm opublikowaniem informacji o ataku w przypadku niezapłacenia okupu, to rzeczywistość, z jaką spotykają się firmy na całym świecie. Niezbędnym elementem wiedzy każdego IOD jest nie tylko zrozumienie, jak i dlaczego te ataki są dokonywane, ale uświadomienie sobie choćby modeli coraz to nowych sposobów ataków phishingowych. Dzięki temu będą oni mogli następnie przekazać tę wiedzę pracownikom podmiotu, w którym pełnią funkcję IOD i na bieżąco aktualizować polityki bezpieczeństwa. W programie przewidziane też zostały praktyczne zajęcia dotyczące sposobu tworzenia bezpiecznych nośników danych, bezpiecznego przesyłania i przechowywania plików w modelach chmurowych czy zagadnienia związane z eIDAS oraz projektowanym jej następcą eIDAS 2.0.

Jakie umiejętności i kompetencje uważacie Państwo za kluczowe dla przyszłych inspektorów ochrony danych, aby skutecznie chronić dane osobowe i zapewniać zgodność z regulacjami? Na jakie aspekty w tym zakresie zwracacie Państwo największą uwagę?

Po pierwsze, głęboka wiedza prawnicza będzie niezbędna, zwłaszcza w kontekście rosnącej liczby regulacji dotyczących danych, takich jak Akt w sprawie sztucznej inteligencji (AI Act), Data Act czy Dyrektywa NIS2. Zrozumienie tych regulacji i ich wpływu na praktyki zarządzania danymi będzie kluczowe.

Po drugie, umiejętność analizy ryzyka i zarządzania nim stanie się coraz bardziej istotna, zwłaszcza w kontekście rosnących zagrożeń cybernetycznych. Inspektorzy będą musieli znać najnowsze techniki i narzędzia służące do identyfikacji i minimalizacji ryzyka, w tym te związane z wykorzystaniem sztucznej inteligencji w systemach bezpieczeństwa. Trzecim kluczowym elementem będą kompetencje techniczne, w tym zrozumienie podstawowych zasad funkcjonowania sztucznej inteligencji, analizy dużych zbiorów danych i cyberbezpieczeństwa. Wiedza ta będzie niezbędna do oceny skuteczności różnych mechanizmów ochrony danych i do zrozumienia, jak nowe technologie mogą wpływać na prywatność i bezpieczeństwo.

8 WSPÓŁPRACA Z UODO

Po pierwsze, głęboka wiedza prawnicza będzie niezbędna, zwłaszcza w kontekście rosnącej liczby regulacji dotyczących danych, takich jak Akt w sprawie sztucznej inteligencji (AI Act), Data Act czy Dyrektywa NIS2. Zrozumienie tych regulacji i ich wpływu na praktyki zarządzania danymi będzie kluczowe.
Po drugie, umiejętność analizy ryzyka i zarządzania nim stanie się coraz bardziej istotna, zwłaszcza w kontekście rosnących zagrożeń cybernetycznych. Inspektorzy będą musieli znać najnowsze techniki i narzędzia służące do identyfikacji i minimalizacji ryzyka, w tym te związane z wykorzystaniem sztucznej inteligencji w systemach bezpieczeństwa.
Trzecim kluczowym elementem będą kompetencje techniczne, w tym zrozumienie podstawowych zasad funkcjonowania sztucznej inteligencji, analizy dużych zbiorów danych i cyberbezpieczeństwa.
Wiedza ta będzie niezbędna do oceny skuteczności różnych mechanizmów ochrony danych i do zrozumienia, jak nowe technologie mogą wpływać na prywatność i bezpieczeństwo.
Czwartą ważną kompetencją będzie zdolność do efektywnej komunikacji i zarządzania zespołem. Inspektorzy będą musieli nie tylko zrozumieć skomplikowane kwestie techniczne i prawne, ale również być w stanie przekazać je w sposób zrozumiały dla różnych działów w organizacji, od IT po zarząd.

Czy macie plany rozwoju programów studiów w zakresie ochrony danych, aby nadążyć za zmieniającymi się potrzebami i wyzwaniami w dziedzinie ochrony danych?
Oczywiście tak. Wymusza to dynamicznie zmieniająca się rzeczywistość prawna i nacisk nałożony przez nas na praktyczny charakter studiów i prezentowanej tematyki. To obejmuje wprowadzenie nowych modułów, które będą skupiać się na zmianach prawodawczych, ale też najnowszych trendach i wyzwaniach technologicznych, takich jak rozwój technologii blockchain czy etycznych aspektach sztucznej inteligencji.

Dlaczego Państwa zdaniem warto podjąć kształcenie w tym zakresie w dzisiejszych czasach?
W dzisiejszym świecie, gdzie dane są często określane jako „nowe złoto", ich ochrona i zarządzanie stały się absolutnie kluczowe dla sukcesu każdej nowoczesnej organizacji. Firmy i instytucje są coraz bardziej świadome tego, że dane nie są tylko aktywem, ale również potencjalnym obszarem ryzyka, co sprawia, że rola inspektora ochrony danych jest ważna i wręcz niezbędna. Studia Podyplomowe w tym zakresie oferują zarówno gruntowne podstawy teoretyczne, jak i praktyczne narzędzia i metody, które są niezbędne do skutecznego zarządzania danymi w dynamicznie zmieniającym się środowisku technologicznym i regulacyjnym.
Nie można też zapomnieć o dynamicznie zmieniającym się krajobrazie legislacyjnym, zarówno na poziomie krajowym, jak i międzynarodowym. Nowe przepisy, takie jak unijny Akt w sprawie sztucznej inteligencji czy Dyrektywa NIS2, wymagają od inspektorów ochrony danych zrozumienia nowych regulacji oraz umiejętności ich praktycznego zastosowania w codziennej pracy. Wreszcie, dokształcanie się w tym zakresie to również sposób na zrozumienie, jakie są najnowsze najlepsze praktyki w zarządzaniu danymi i jak można je efektywnie wdrożyć w swojej organizacji. To kompetencje, które są cenione tak w sektorze prywatnym, jak i w instytucjach publicznych, co otwiera szerokie perspektywy zawodowe dla tych, którzy zdecydują się na taką ścieżkę kariery.

8 WSPÓŁPRACA Z UODO

KOMENTARZ

mgr Sławomir Jagieła EMBA, DBA. Dyrektor Kolegium Kształcenia Podyplomowego
Członek Rady Biznesu Akademii Ekonomiczno-Humanistycznej w Warszawie

Program studiów ma na celu przygotowanie uczestników do zawodu Inspektora Ochrony Danych (IOD) oraz umożliwienie zdobycia niezbędnych umiejętności i wiedzy związanych z ochroną danych. Celem studiów jest także zapewnienie uczestnikom pełnego zrozumienia przepisów dotyczących ochrony danych, w tym tak istotnych regulacji jak RODO w Polsce i na terenie Europy, a także równoważnych przepisów i uregulowań obowiązujących w innych krajach. Dodatkowo, program studiów podyplomowych umożliwia zdobycie umiejętności z zakresu przeprowadzania audytów i kontroli, co ma szczególne znaczenie, gdyż Inspektorzy Ochrony Danych często odpowiadają za nadzór i audyty w organizacjach. Nasz program edukacyjny przygotuje uczestników do skutecznego wykonywania tych kluczowych zadań.

W celu ciągłego dostosowywania programu edukacyjnego do dynamicznie zmieniającego się środowiska regulacyjnego i biznesowego, Akademia Ekonomiczno-Humanistyczna w Warszawie stale monitoruje zmiany w przepisach i regulacjach dotyczących ochrony danych, dostosowując swoje programy na podstawie nowych wymagań prawnych.

Dodatkowo, przeprowadzamy konsultacje z ekspertami z obszaru ochrony danych oraz prawnikami, aby pozyskać wgląd w najnowsze wyzwania i trendy w tej dziedzinie.

Jednocześnie wykorzystujemy aktualne studia przypadków i przykłady z rzeczywistego życia, które pomagają uczestnikom studiów podyplomowych zrozumieć, jakie wyzwania mogą napotykać organizacje w zakresie ochrony danych oraz jakie rozwiązania mogą być stosowane.

Akademia Ekonomiczno-Humanistyczna w Warszawie współpracuje również z Urzędem Ochrony Danych Osobowych, aby zapewnić, że programy edukacyjne studiów podyplomowych są praktyczne i dostosowane do aktualnych potrzeb.

Dostosowywanie programów edukacyjnych w zakresie ochrony danych do dynamicznie zmieniającego się środowiska regulacyjnego i biznesowego jest kluczowe, aby zagwarantować, że absolwenci tych programów są odpowiednio przygotowani do pracy w tym obszarze.

Przy wyborze studiów z zakresu ochrony danych osobowych istnieje kilka kluczowych aspektów, które warto uwzględnić, aby podjąć najlepszą decyzję dotyczącą wyboru programu edukacyjnego.

8 WSPÓŁPRACA Z UODO

Po pierwsze, zaleca się sprawdzenie renomy uczelni i upewnienie się, że wybrana uczelnia cieszy się dobrą reputacją oraz uznaniem jako miejsce o wysokim standardzie nauczania. Renomowane placówki edukacyjne często oferują bardziej zaawansowane i kompleksowe możliwości edukacyjne, a także nadają dyplomom większą wartość.

Następnie, warto szczegółowo zapoznać się z programem studiów oferowanym przez uczelnię w celu upewnienia się, że program obejmuje istotne zagadnienia związane z ochroną danych osobowych, takie jak przepisy prawne, technologie, zarządzanie ryzykiem i audyt. Warto sprawdzić, czy program studiów jest wspierany przez instytucje o renomie, na przykład Urząd Ochrony Danych Osobowych, co może dodatkowo świadczyć o jakości edukacji.

Dla przyszłych studentów zainteresowanych studiami z zakresu ochrony danych osobowych, zaleca się również dokładną weryfikację doświadczenia i kwalifikacji kadry dydaktycznej. Ważne jest, aby wykładowcy posiadali praktyczne doświadczenie zawodowe oraz byli w stanie przekazać cenne wskazówki i wiedzę w dziedzinie ochrony danych uczestnikom studiów podyplomowych.

Należy pamiętać, że wybór programu studiów z zakresu ochrony danych osobowych to istotna decyzja, która może znacząco wpłynąć na przyszłą karierę uczestnika studiów podyplomowych. Dlatego warto poświęcić czas na dokładne rozważenie wszystkich dostępnych opcji i dostosować wybór do swoich celów zawodowych oraz zainteresowań. Kształcenie w obszarze ochrony danych niesie za sobą wiele istotnych korzyści i stanowi cenny aspekt w dzisiejszym świecie. Pomaga rozwijać umiejętność krytycznego myślenia, umożliwiając jednocześnie zdobywanie kompetencji w analizie informacji oraz podejmowaniu trafnych decyzji. W szczególności w epoce informacyjnej, w której jesteśmy bombardowani ogromną ilością danych i różnorodnymi opiniami, umiejętność ta nabiera kluczowego znaczenia.

Kształcenie w dziedzinie ochrony danych wpływa również na zwiększenie konkurencyjności na rynku pracy. Wykształcenie może znacząco przyczynić się do zdobycia lepszych stanowisk zawodowych oraz podniesienia poziomu wynagrodzenia. Wielu pracodawców oczekuje od swoich pracowników odpowiedniego wykształcenia i kompetencji w zakresie ochrony danych, co sprawia, że posiadanie takiej edukacji staje się kluczowym atutem. Ponadto, ciągłe doskonalenie wiedzy i umiejętności jest niezwykle istotne, aby pozostać na bieżąco i dostosować się do dynamicznie zmieniającego się otoczenia. Edukacja pozwala na śledzenie najnowszych trendów, technologii oraz aktualnych przepisów prawnych, co jest nieodzowne w dzisiejszym środowisku biznesowym i społecznym.

URZĄD OCHRONY DANYCH OSOBOWYCH