JUSTYNA JABŁONKA

Maj 2023
Nr 3/2023

KANCELARIA WYRZYKOWSCY

Newsletter
INSPEKTORA OCHRONY DANYCH
ADW. JUSTYNY JABŁONKI

Szanowni Państwo,

w majowym Newsletterze IOD przeczytacie nie tylko o kwestiach spędzających sen z powiek z zakresu danych osobowych, tj. udostępniać czy nie udostępniać? -> w przedmiocie danych, o które wnioskuje Policja bądź zgłaszać czy nie zgłaszać? -> w związku z procedurą zgłaszania naruszeń do PUODO. W tym numerze zdecydowałam się również umieścić wypowiedź Adama Wyrzykowskiego, który swe zainteresowania wiąże z tematyką AI, prawem nowych technologii, dotyczącą Sztucznej Inteligencji i zastosowania jej w pracy urzędnika. Sama natomiast postanowiłam skupić się w tym wydaniu na 27 pytaniach o IOD, po co? – więcej na str. 2©

Przyjemnej lektury.

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

Tematy majowe:

I. 27 pytań do Administratora o IOD. Kto i w jakim celu je zadał?

Prezes Urzędu Ochrony Danych osobowych skierował do poszczególnych Administratorów danych listę pytań dotyczącą współpracy z Inspektorem Ochrony Danych – IOD. Pytania te trafiły do podmiotów z sektora prywatnego i publicznego.

Lista zadanych 27 pytań przedstawia się następująco:

1.Czy u administratora został wyznaczony inspektor ochrony danych (IOD)?
2. Czy na administratorze ciąży obowiązek wyznaczenia IOD (jeżeli tak, to na jakiej podstawie prawnej), czy też IOD został wyznaczony mimo braku takiego obowiązku?
3. Czy administrator opublikował imię i nazwisko oraz kontakt do IOD na swojej stronie internetowej lub - jeżeli nie prowadzi swojej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia swojej działalności?
4. Czy ww. informacje znajdują się w ogólnie dostępnym miejscu (proszę wskazać to miejsce, w przypadku strony internetowej proszę wskazać jej adres oraz link do tej informacji)?
5. Czy Inspektor Ochrony Danych jest pracownikiem administratora, a jeśli nie, to na jakiej podstawie prawnej wykonuje swoje obowiązki?
6. Czy IOD został powołany na wyłączność u administratora, czy wykonuje swoje obowiązki również u innych administratorów?
7. Na podstawie jakich kwalifikacji administrator wyznaczył IOD (np. wykształcenie, doświadczenie, wiedza)?
8. Jakie niezbędne zasoby, o których mowa w art. 38 ust. 2 rozporządzenia 2016/679 administrator zapewnia IOD?
9. W jaki sposób administrator zapewnia zasoby na utrzymanie wiedzy fachowej IOD?
10. Jakie stanowisko zajmuje IOD i komu podlega w strukturze organizacyjnej administratora?
11. Czy administrator powołał zastępcę IOD, jeżeli tak, to kiedy?
12. Czy u administratora funkcjonuje zespół IOD lub inna forma stałego wsparcia IOD w zakresie wykonywania jego zadań?
13. W jaki sposób administrator zapewnia by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (np. czy zostały opracowane zasady dotyczące tego, jakie sprawy mają być konsultowane z IOD, kto i w jakich sytuacjach powinien zgłaszać się w celu uzyskania konsultacji IOD, czy i na jakich zasadach IOD bierze udział w naradach kierownictwa)
14. W jaki sposób administrator zapewnia IOD dostęp do danych osobowych i operacji przetwarzania?

15. Czy administrator przyjął jakiekolwiek regulacje wewnętrzne dotyczące funkcjonowania IOD (w szczególności w celu zapewnienia poszanowania gwarancji jego niezależności oraz jego uprawnień w zakresie dostępu do danych osobowych i operacji przetwarzania, włączania we wszystkie sprawy dotyczące ochrony danych osobowych, unikania konfliktu interesów), a jeżeli tak, to w jakim akcie wewnętrznym zostały one przewidziane?
16. W jaki sposób administrator zapewnia, aby IOD nie były wydawane instrukcje co do wykonywania zdań przez IOD?
17. W jaki sposób administrator zapewnia, aby IOD nie były karany i odwoływany za wykonywanie swoich zadań?
18. W jaki sposób ADO postępuje w przypadku, gdy nie uwzględnia wskazówek lub rekomendacji IOD, np. czy dokumentuje powody niezastosowania tych wskazówek?
19. W jaki sposób osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych zgodnie z art. 38 ust. 4 rozporządzenia 2016/679?
20. Czy inspektor ochrony danych wykonuje również inne obowiązki lub sprawuje inną funkcję poza obowiązkami związanymi z ochroną danych osobowych, jeżeli tak to:
a. jakie oraz w jakim wymiarze czasu pełni funkcję IOD, a w jakim inne zadania,
b. w jaki sposób administrator ocenił, że w przypadku każdego z tych zadań nie występuje konflikt interesów, o którym mowa w art. 38 ust 6 rozporządzenia 2016/679 ?
c. czy w zakresie wykonywania innych zadań IOD podlega innym osobom niż najwyższe kierownictwo administratora?
21. Czy administrator opracował politykę zarządzania konfliktem interesów lub wprowadził inny mechanizm zapewniający niewystępowanie konfliktu interesów?
22. Czy IOD wykonuje swoje zadania jedynie w siedzibie administratora, a jeżeli nie, to w jakim miejscu i w jaki sposób zapewniona jest stała dostępność IOD dla kierownictwa i pracowników administratora?
23. Czy IOD opracował (systematycznie opracowuje) plan swojej pracy np. w zakresie szkoleń, audytów?
24. Czy taki plan był prezentowany administratorowi w celu umożliwienia dokonania oceny, czy IOD dysponuje wystarczającymi zasobami i uprawnieniami w obszarach, które IOD obejmuje swoimi zadaniami?
25. Jak często i w jaki sposób IOD przekazuje administratorowi wyniki przeprowadzonych audytów?
26. Czy administrator występował do IOD o udzielenie zaleceń co do oceny skutków dla ochrony danych, a jeśli tak, to w jakich sytuacjach?
27. Czy administrator kontroluje pracę inspektora, jeżeli tak, to w jaki sposób?

Jak ważna jest rola Inspektora Ochrony Danych w organizacji, myślę, że każdy z Państwa kto konsultuje ze mną poszczególne umowy, regulaminy, procedury, już wie. IOD powinien być niezależny i odpowiednio zaangażowany we wszystkie sprawy związane z ochroną danych osobowych.

Przez ostatnie lata organ nadzorczy przeprowadzał liczne kontrole mające na celu sprawdzenie, czy administratorzy przestrzegają wymogów dotyczących IOD. W większości przypadków kontrole te zakończyły się pozytywnie, jednak pojawiły się również nieprawidłowości, które wymagały podjęcia działań naprawczych. Jednym z głównych problemów, który występował, było niedostateczne uwzględnienie konfliktu interesów związanych z pełnieniem funkcji IOD. W niektórych przypadkach IOD pełnił swoje obowiązki jednocześnie będąc sekretarzem gminy, co stwarzało konflikt interesów. Ponadto, niekiedy administratorzy podejmowali operacje przetwarzania danych osobowych bez wcześniejszej konsultacji z IOD, co również naruszało przepisy.

To, na co ja, jako IOD, zwracam szczególną uwagę to kwestia odpowiedniej organizacji współpracy Administratora z IOD. Ważne jest to zwłaszcza u Administratora, gdzie jego dobra organizacja pracy wymaga podziału na szereg wydziałów, stanowisk samodzielnych. Otóż, w mojej opinii, kierownicy tychże wydziałów, osoby na samodzielnych stanowiskach powinny tworzyć wraz z IOD zespół ochrony danych u danego Administratora, tj. stanowić formę stałego wsparcia dla IOD w zakresie wykonywania jego zadań (pyt. nr 12).

Dotyczy to zwłaszcza większych jednostek – Urzędów Gmin/Miast, gdzie mamy do czynienia z szeregiem procesów przetwarzania danych, poszczególne decyzje zapadają niekiedy bardzo szybko i różne osoby są odpowiedzialne za kolejne etapy w realizowaniu projektów. Osoba, która odgrywa również znaczącą rolę w działalności jednostki to zaplecze IT, które posiada informacje ważne w zakresie prawidłowego zabezpieczenia danych. Zatem, osoba ta również powinna zostać włączona w skład zespołu IOD.

Jak wskazuje Jacek Młotkiewicz, dyrektor Departamentu Kontroli i Naruszeń w UODO, w Biuletynie UODO Nr 2/04/23: *„Listę 27 pytań administratorzy wykorzystywali do autokontroli w zakresie realizacji swoich obowiązków odnoszących się do zagwarantowania IOD właściwej pozycji i prawidłowego wykonywania zadań. W czasie prowadzonych postępowań stwierdzono liczne nieprawidłowości dotyczące*

powołania i funkcjonowania inspektorów ochrony danych, które dotyczą takich kwestii, jak np.:

1. *niewłaściwe włączanie IOD w sprawy dotyczące ochrony danych osobowych,*
2. *niepodejmowanie działań mających na celu zapewnienie inspektorowi ochrony danych zasobów niezbędnych do utrzymania jego wiedzy fachowej,*
3. *brak procedur zapewniających niezależność inspektora ochrony danych, w szczególności dotyczących zakazu otrzymywania instrukcji, wydawania poleceń, jak również zapewnienia, że w ramach wykonywania zadań inspektora ochrony danych nie będzie on odwoływany ani karany.*

Wiele z naszych zastrzeżeń związanych też było z nałożeniem na inspektorów ochrony danych zadań, które należą do obowiązków administratorów, jak np. prowadzenie rejestru czynności przetwarzania, rejestru naruszeń ochrony danych osobowych czy tworzenia wewnętrznych polityk.

Inspektor nie może bowiem być obciążony działaniami, które ma oceniać pod kątem ich zgodności z przepisami prawa i regulacjami wewnętrznymi administratora."

Źródło: Biuletyn UODO Nr 2/04/23, rozmowa z Ekspertem: Jackiem Młotkiewiczem, str. 10 Biuletynu.

Autor:
Justyna Jabłonka
Inspektor Ochrony Danych
adwokat

Wyciąg z przepisów:

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.): RODO:

I. **Artykuł 37 RODO: Wyznaczenie inspektora ochrony danych**

1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, **zawsze, gdy:**

a. przetwarzania dokonują **organ lub podmiot publiczny**, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b. główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

c. główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.

2. Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

3. Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć - z uwzględnieniem ich struktury organizacyjnej i wielkości - jednego inspektora ochrony danych.

4. W przypadkach innych niż te, o których mowa w ust. 1, administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych. Inspektor ochrony danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające.

5. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.

6. Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

7. Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

II. Artykuł 38 RODO: Status inspektora ochrony danych

1. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

2. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

3. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

4. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.

5. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań - zgodnie z prawem Unii lub prawem państwa członkowskiego.

6. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych:

Artykuł 11: Udostępnianie danych inspektora ochrony danych

Podmiot, który wyznaczył inspektora, udostępnia dane inspektora: imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

II. Sztuczna Inteligencja w pracy urzędnika.

Czy tego chcemy czy nie sztuczna inteligencja nie zniknie… i choćbyśmy rzucali w nią kamieniami tak jak kiedyś rzucano w maszyny parowe to nie wyprzemy z naszego życia tej niezwykle szybko rozwijającej się technologii, która dotykać będzie coraz więcej aspektów naszego życia w tym również pracy urzędnika.

Czym jest sztuczna inteligencja?

Sztuczna Inteligencja (SI), znana też jako AI (od ang. Artficial Inteligencje) to w dużym uproszczeniu zdolność maszyn, programów komputerowych, modelów językowych do wykazywania ludzkich umiejętności, takich jak rozumowanie, uczenie się, planowanie i kreatywność. Jest to gałąź informatyki skoncentrowana na tworzeniu systemów zdolnych do wykonywania zadań, które zwykle wymagają ludzkiego intelektu. Wykorzystuje uczenie maszynowe i głębokie sieci neuronowe. Jest w stanie przetwarzać ogromne ilości danych i uczyć się na podstawie doświadczeń.
AI z całą pewnością zmieni nasz świat na różnych płaszczyznach – od medycyny, przez biznes aż po prace urzędów.

Dlaczego?

AI może przekształcić sposób w jaki funkcjonują urzędy gminne umożliwiając skuteczniejsze i efektywniejsze zarządzanie zasobami. Sztuczna inteligencja znacznie usprawni zarządzanie danymi, analizę procesów, które wcześniej zajmowały urzędnikom wiele godzin. Na przykład system AI mogą automatycznie sortować i analizować wnioski, skargi i prośby od mieszkańców przyspieszając procesy decyzyjne.
Systemy oparte o sztuczną inteligencją mogą na przykład znacząco wspomóc pracę w pisaniu wniosków o dotacje czy tez wnieść znaczący wkład proces kreatywny w tworzeniu nowoczesnych rozwiązań dla mieszkańców gminy.

Przykładem takiego narzędzia jest chociażby bardzo popularny ChatGPT, który jest modelem językowym opracowanym przez OpenAI. Został zaprojektowany do generowania tekstu i może prowadzić rozmowy na różne tematy, opowiadając na pytania, pisząc artykuły, tworząc historie i wykonując wiele innych zadań związanych z językiem.

Ograniczając się jedynie do tego narzędzia już mamy ogrom możliwości, które urzędnik, nauczyciel, pracownik jednostki samorządowej może wykorzystać aby lepiej przygotować się do swojej pracy.

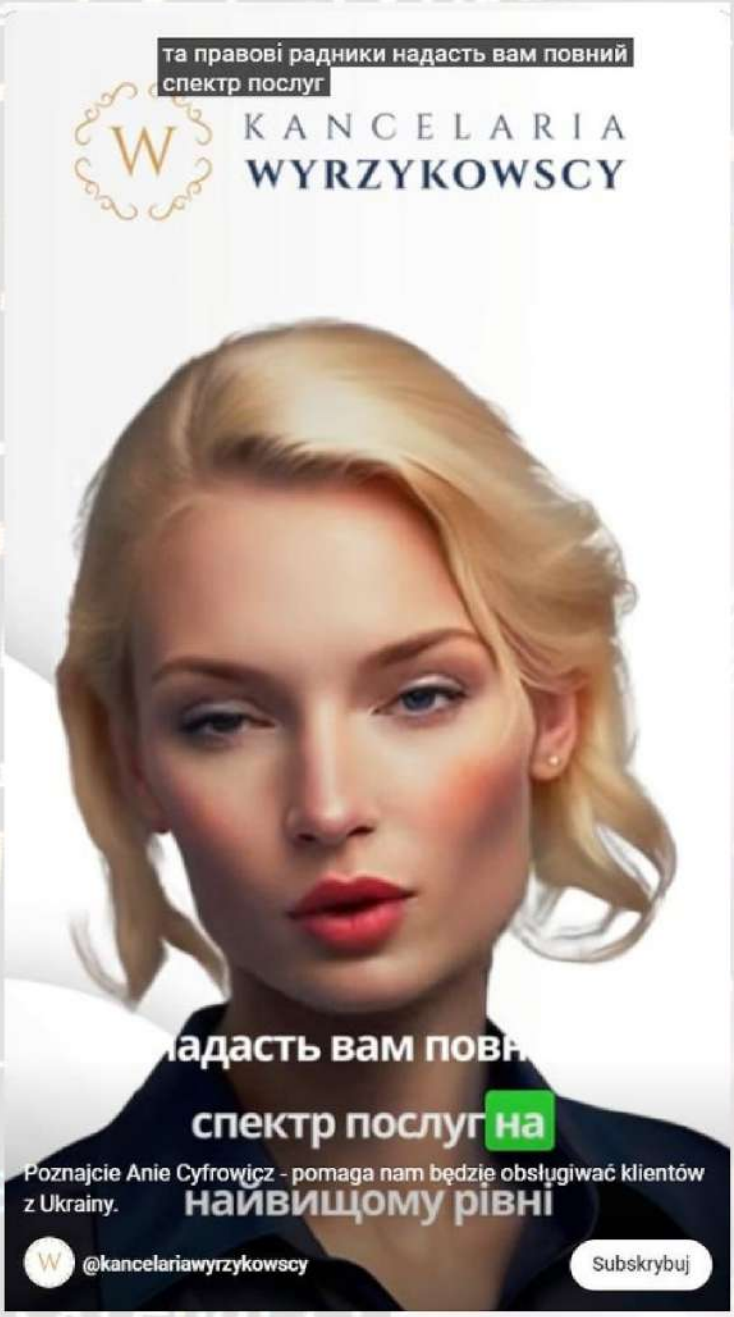
Nauczyciel aby lepiej przygotować się do lekcji może wspomagać się tworzeniem kreatywnych zadań, historii, testów, gier i zabaw, które uczą.

Urzędy mogą używać zaawansowanych technologii AI do komunikacji z mieszkańcami zwłaszcza używając chatbotów i awatarów, które mogą lepiej komunikować się za pośrednictwem stron urzędowych np. z osobami niepełnosprawnymi czy też obcokrajowcami. Przykład: osoба niedowidząca wchodząc na stronę urzędu nie musi czytać tekstu wystarczy, że w rozmowie z awatarem urzędnika przedstawi swój problem a on poda rozwiązanie. Takie możliwości już istnieją.

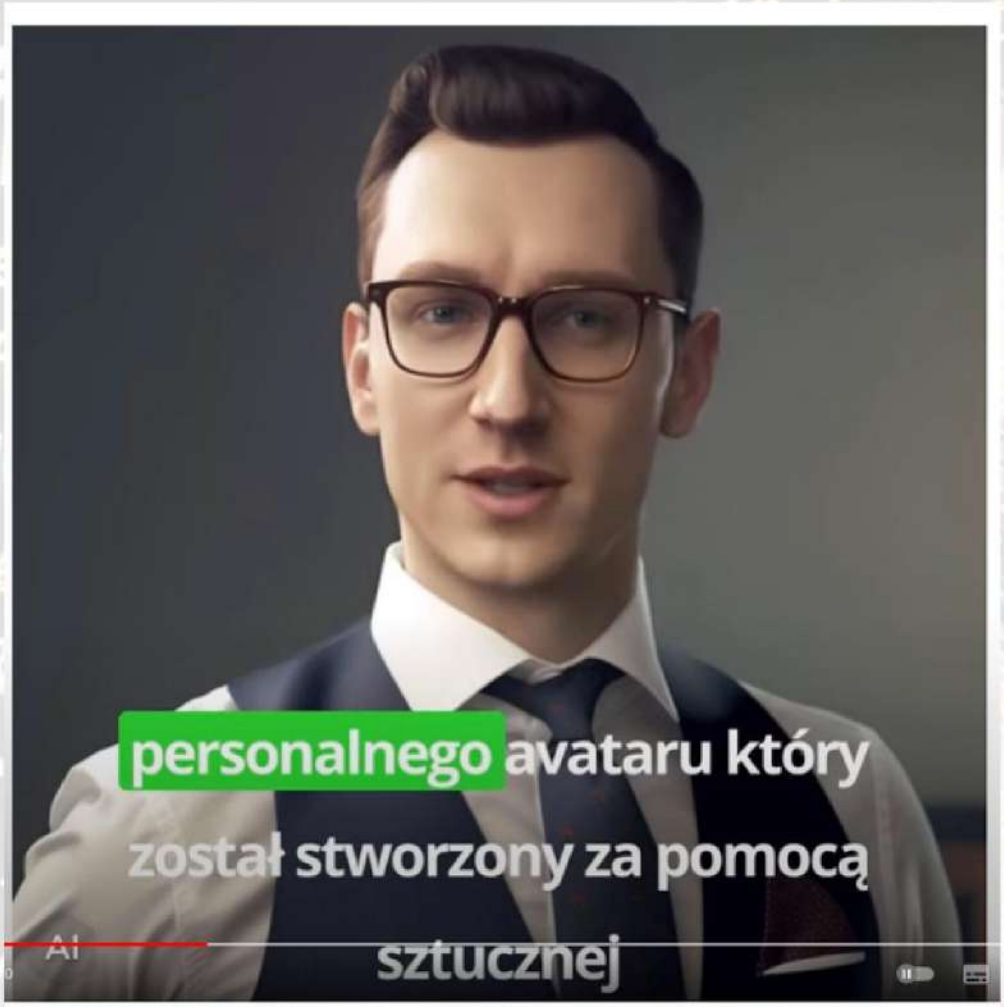
Oczywiście sztuczna inteligencja to konieczność, naszym zdaniem, powstania ram prawnych i również ogromne pole do nadużyć ale nie o tym w dzisiejszym wpisie.

Poniżej przedstawiamy dwa przykłady zastosowania awatarów opartych o AI:
Pierwszy przykład to Ania Cyfrowicz, która pomaga Kancelarii w obsłudze klientów z Ukrainy:

https://www.youtube.com/shorts/DI8iKBdPcK8



Drugi przykład to idea wykorzystywania indywidualnych awatarów do obsługi różnych procesów:



W niniejszym artykule naszą intencją było zasygnalizować Państwu jak wielkie znaczenie będzie miała w najbliższych latach sztuczna inteligencja. Jeśli podoba się Państwu nasz newsletter i tematy, które poruszamy prosimy dodać do obserwowanych:

https://www.facebook.com/kancelariawyrzykowscy

Autor:
Adam Wyrzykowski
doradca podatkowy
Partner Zarządzający w Kancelarii
Wyrzykowscy

III. Udostępnienie danych osobowych na żądanie Policji

Obowiązek udostępnienia danych osobowych Policji

Jednostki samorządu terytorialnego i ich jednostki organizacyjne mają obowiązek udzielania pomocy Policji i organom prowadzącym postępowanie karne. Obowiązek ten wynika w szczególności z treści art. 15 § 2 Kodeksu postępowania karnego, który stanowi, że wszystkie instytucje państwowe i samorządowe są obowiązane w zakresie swego działania do udzielania pomocy organom prowadzącym postępowanie karne w terminie wyznaczonym przez te organy. W odniesieniu do Policji zakres obowiązku udzielania pomocy doprecyzowuje art. 15 ust. 1 pkt 6 ustawy o Policji, zgodnie z którym Policjanci wykonując swoje czynności, mają prawo żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej, zaś instytucje, organy i przedsiębiorcy są obowiązani do udzielenia tej pomocy w zakresie swojego działania. Elementem wskazanego obowiązku jest konieczność udostępniania na żądanie Policji danych osobowych. Art. 20 ust. 1d zd. 3 ustawy o Policji jednoznacznie stanowi, że służby, instytucje państwowe oraz organy władzy publicznej są obowiązane do nieodpłatnego udostępnienia Policji informacji, w tym także danych osobowych.

Udostępnienie danych osobowych Policji a RODO

Udostępnianie danych osobowych jest formą ich przetwarzania. Administrator zobowiązany do udostępnienia danych osobowych wykonuje ciążący na nim obowiązek prawny, a więc podstawą jego działania w tym zakresie jest art. 6 ust. 1 lit. c RODO. Oznacza to, że udostępnienie danych osobowych Policji nie wymaga zgody osoby, której dane dotyczą. Co więcej, zgodnie z przepisami ustawy o Policji, przetwarzanie danych osobowych przez Policję może mieć charakter niejawny i odbywać się bez wiedzy, osoby, której dane dotyczą.

Informacje, których może żądać Policja

Zgodnie z art. 20 ust. 1d zd. 4 ustawy o Policji, Policja może uzyskiwać informacje gromadzone przez służby, instytucje państwowe oraz organy władzy publicznej w administrowanych przez nie zbiorach danych lub rejestrach. Zakres danych, których może żądać Policja jest w zasadzie nieograniczony. Art. 20 ust. 1c ustawy o Policji wprost wskazuje, że jest ona upoważniona do przetwarzania danych wrażliwych, o których mowa w art. 9 RODO. Co przy tym istotne, Policja może żądać udostępnienia danych osobowych nie tylko do celów związanych z zapobieganiem i zwalczaniem przestępczości, ale także np. w związku z prowadzeniem postępowań administracyjnych czy realizacją czynności administracyjno-porządkowych.

Jedynym wyraźnym ograniczeniem w tym zakresie jest brak możliwości przetwarzania przez Policję do celów, które nie są związane z zapobieganiem i zwalczaniem przestępczości danych dotyczących kodu genetycznego. W konsekwencji administrator nie ma zbyt dużych możliwości kwestionowania zakresu danych osobowych, których udostępnienia żąda Policja. Jednocześnie należy jednak pamiętać o wynikających z przepisów RODO zasadach celowości i adekwatności danych. Wymagają one, aby Policja występowała z żądaniem udostępnienia tych danych, które są niezbędne do realizacji określonego celu. W przypadku wątpliwości co do zakresu żądanych przez Policję danych osobowych, administrator powinien zwrócić się o uzasadnienie potrzeby ich udostępnienia.

Wniosek o udostępnienie danych osobowych i tryb udostępnienia

Sposób żądania przez Policję udostępnienia danych osobowych nie jest precyzyjnie określony. Pewne znaczenie mogą mieć tu przepisy rozdziału 6 Rozporządzenia Rady Ministrów z dnia 4 lutego 2020 r. w sprawie postępowania przy wykonywaniu niektórych uprawnień policjantów. Przewidują one m.in., że organ Policji lub policjant działający z upoważnienia tego organu doręcza żądanie udzielenia niezbędnej pomocy lub przekazuje je drogą elektroniczną oraz że żądanie udzielenia niezbędnej pomocy powinno zawierać powołanie podstawy prawnej żądania, określenie rodzaju i zakresu niezbędnej pomocy oraz wskazanie policjanta korzystającego z pomocy. Należy przyjąć, że niedopełnienie wymogów formalnych żądania (w tym np. wskazanie niewłaściwej podstawy prawnej żądania), samo w sobie nie będzie w każdym przypadku uzasadniało odmowy udostępnienia Policji żądanych przez nią danych osobowych. W określonych

przypadkach nie można wykluczać nawet udostępnienia danych osobowych na podstawie ustnego żądania Policjanta, zwłaszcza w sytuacjach związanych z działaniem w stanie wyższej konieczności.

W każdym przypadku administrator jest zobowiązany do zweryfikowania tożsamości osoby, która występuje z żądaniem udostępnienia danych osobowych. W tym zakresie trzeba mieć na względzie problemy z potwierdzeniem tożsamości osoby kierującej wniosek w formie elektronicznej. Z uwagi na pojawiające się wątpliwości co do bezpieczeństwa wykorzystania podpisu zaufanego i podpisu osobistego, należy rekomendować, aby dane osobowe były udostępniane tylko na podstawie wniosków elektronicznych opatrzonych podpisem kwalifikowanym. Co do zasady należy też dążyć do wyeliminowania praktyki polegającej na udostępnianiu danych osobowych przez telefon.

Jednocześnie warto zwrócić uwagę, na wynikający z § 26 wskazanego rozporządzenia, obowiązek sporządzenia przez Policjanta pisemnego pokwitowania na rzeczy lub dokumenty użyczone w ramach pomocy. Mając na względzie ciążący na administratorze obowiązek rozliczalności w zakresie prawidłowości przetwarzania danych, warto by administrator, który przekazuje Policji dokumenty lub nośniki zawierające dane osobowe takie pokwitowanie uzyskał.

Policja nie jest odbiorcą danych osobowych

Zgodnie z art. 4 pkt 9 RODO organy publiczne, które na podstawie przepisów prawa mogą otrzymywać dane osobowe w ramach konkretnego postępowania, nie są uznawane za odbiorców danych osobowych. Oznacza to m.in., że nie ma obowiązku wskazywania Policji jako odbiorcy danych w klauzuli informacyjnej w ramach obowiązku, o którym mowa w art. 13 ust. 1 lit. e i art. 14 ust. 1 lit. e RODO; że nie ma obowiązku wskazywania Policji jako odbiorcy danych w rejestrze czynności przetwarzania oraz, że nie ma obowiązku informowania osoby, której dane dotyczą w oparciu o art. 15 ust. 1 lit. c RODO o udostępnieniu danych Policji

Konsekwencje nieudostępnienia danych osobowych na żądanie Policji

Nieuzasadniona odmowa udostępnienia danych osobowych na żądanie Policji może być podstawą odpowiedzialności karnej za przestępstwo niedopełnienia obowiązków przez funkcjonariusza publicznego, za które zgodnie z art. 231 § 1 Kodeksu karnego grozi kara pozbawienia wolności do lat 3. Z drugiej strony udostępnienie danych osobowych z naruszeniem zasad ich przetwarzania, w tym w szczególności udostępnienie danych osobie nieuprawnionej naraża administratora danych na odpowiedzialność administracyjną na podstawie przepisów RODO.

Autor:
Grzegorz Lubeńczuk
zespół Inspektora Ochrony Danych
radca prawny

IV. Naruszenie ochrony danych osobowych - zgłaszać czy nie?

Kara dla administratora danych za brak zgłoszenia naruszenia, czyli o tym, dlaczego przeprowadzenie analizy ryzyka i skutków związanych z naruszeniem ochrony danych osobowych oraz zgłoszenie tego naruszenia do UODO ma tak istotne znaczenie.

Prezes UODO po raz kolejny nałożył karę na administratora za brak zgłoszenia naruszenia ochrony danych osobowych. Tym razem, karę otrzymała Prokuratur Rejonowa, a jej wysokość to 20.000 zł.

Ale zacznijmy od początku. Jak to jest z tym naruszeniem i obowiązkiem jego zgłoszenia?

Zgodnie z art. 4 pkt 12 RODO, naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Z kolei art. 33 RODO stanowi, że w przypadku naruszenia ochrony danych osobowych, administrator danych bez zbędnej zwłoki, jednakże nie później niż w terminie 72 godzin od powzięcia wiedzy o naruszeniu, zgłasza ten fakt do organu nadzorczego. Wyjątkiem jest sytuacja, kiedy naruszenie nie niesie za sobą skutków dla praw lub wolności osób, których dane dotyczą. Zgodnie z kolejnym przepisem – art. 34 RODO, jeśli naruszenie pociąga za sobą wysokie ryzyko negatywnych skutków dla praw i wolności osób, których dane dotyczą, administrator ma obowiązek powiadomić także osoby, których dane zostały naruszone.

Czemu ma służyć takie zgłoszenie? Według Prezesa UODO, zgłaszanie naruszeń ochrony danych osobowych przez administratorów stanowi skuteczne narzędzie przyczyniające się do realnej poprawy bezpieczeństwa przetwarzania danych osobowych.

Skąd mamy jednak wiedzieć, czy naruszenie stanowi ryzyko dla praw i wolności osób trzecich i mamy obowiązek je zgłosić?
Administrator powinien dokonać oceny ryzyka naruszenia praw lub wolności osoby fizycznej, która powinna być przeprowadzona przede wszystkim przez pryzmat osoby zagrożonej. Aby to uczynić i to w sposób prawidłowy, administrator musi posiadać jednak szczegółowe informacje w przedmiocie naruszenia.

Dla przypomnienia, warto wskazać, że aby umożliwić administratorowi przeprowadzenie analizy ryzyka i podjęcie decyzji co do tego, czy naruszenie podlega zgłoszeniu do UODO, trzeba być szczególnie czujnym i uważnym np. w sytuacjach:

- uzasadnionego przypuszczenia o nieupoważnionej modyfikacji danych osobowych, w której skład wchodzi: dopisywanie, usuwanie, aktualizacja, niszczenie całkowite bądź częściowe informacje,
- odkrycia śladów włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych,
- odkrycia śladów włamania lub próby włamania do szafek, w których przechowywane są – w postaci papierowej lub elektronicznej – nośniki danych osobowych,
- zagubienia bądź kradzieży nośnika danych osobowych, (płyty CD, pendrive`a, komputera przenośnego, dysku itp.),
- kradzieży sprzętu informatycznego, w którym przechowywane są dane,
- fizycznego zniszczenia lub podejrzenia zniszczenia elementów systemu informatycznego,
- nieprawidłowych zachowań osób, które przetwarzają dane, poprzez naruszenie zasady czystego ekranu, czystego biurka, bezpiecznego pomieszczenia, brak wylogowania się z komputera przy opuszczeniu stanowiska służbowego,
- zbyt niskiej lub zbyt wysokiej temperatury, która może uszkodzić sprzęty, na których przetwarzane są dane osobowe,
- zawieszania się systemu,
- błędów oprogramowania lub błędy sprzętu,
- braku możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych,
- znacznego spowolnienia systemu informatycznego, pojawienia się niestandardowych komunikatów generowanych przez system informatyczny,
- informacji z systemu antywirusowego o zainfekowaniu bądź naruszeniu zabezpieczeń systemu informatycznego wirusami.

To oczywiście jedynie przykładowe sytuacje, ale okazuje się, że występują dość często i w praktyce mogą mieć duży wpływ na bezpieczne przetwarzanie danych.

Jak dokonać zgłoszenia naruszenia administratorowi, aby umożliwić mu przeprowadzenie analizy zagrożenia? Najlepiej jest jak najdokładniej opisać zdarzenie, uwzględniając odpowiedzi na pytania: **co? jak? kiedy? kto? gdzie?**

Niezwykle ważnym jest, aby zgłosić administratorowi naruszenie, lub wątpliwość co do tego, czy doszło do naruszenia, jak najszybciej, albowiem sam administrator ma jedynie **72 godziny (od momentu powzięcia informacji o naruszeniu)** na to, aby dokonać zgłoszenia do organu nadzorczego. Doświadczenie pokazuje natomiast, że to **bardzo mało czasu i trzeba go dobrze wykorzystać.**

Wracając do naszej historii, dlaczego Prezes UODO nałożył karę na Prokuraturę Rejonową?

Do UODO wpłynęła informacja wskazująca na możliwość wystąpienia naruszenia ochrony danych osobowych w Prokuraturze Rejonowej, które miało polegać na tym, iż przekazano dziennikarzowi, w odpowiedzi na jego wniosek o udostępnienie informacji publicznej, dokumentację z niezanonimizowanymi danymi osób. Dziennikarz z kolei, dane te upublicznił w internecie. W związku z tym, że Prokuratura Rejonowa nie zgłosiła naruszenia do UODO, UODO wszczął postępowanie z urzędu, na skutek informacji o zdarzeniu. Kara nałożona została dlatego, że jak ustalono w trakcie postępowania, Prokuratura Rejonowa nie tylko nie zgłosiła naruszenia do UODO i nie zawiadomiła osób, których dane dotyczyły o naruszeniu, ale także nie przeprowadziła żadnej analizy ryzyka w tym zakresie. Co ważne, Prezes UODO uznał, że obowiązek zgłoszenia naruszenia nie jest wcale zależny od tego, czy zagrożenie dla osób, których dane dotyczą faktycznie się uskuteczniło.

Prezes UODO powołał się na obszerne już w tym temacie orzecznictwo sądów administracyjnych, które jednoznacznie wskazuje, że „(...)samo wystąpienie naruszenia ochrony danych osobowych, z którym wiąże się ryzyko naruszenia praw lub wolności osób fizycznych, implikuje obowiązek zgłoszenia naruszenia właściwemu organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych" – tak m. in. wypowiedział się Wojewódzki Sąd Administracyjny w Warszawie w uzasadnieniu wyroku z dnia 22 września 2021 r., sygn. akt II SA/Wa 791/21. To treść jednego z wielu orzeczeń, jednakże linia orzecznicza jest tutaj jednorodna. Bez znaczenia jest również fakt, iż dane zostały udostępnione jednej zidentyfikowanej osobie. Dane bowiem zostały udostępnione nieuprawnionej osobie, co oznacza, że nastąpiło naruszenie bezpieczeństwa prowadzące do nieuprawnionego ujawnienia danych osobowych.

A co miało wpływ na wymiar nałożonej kary?

Prezes UODO nakładając karę wziął pod uwagę:

- Charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody,
- Umyślny charakter naruszenia, gdzie umyślność „obejmuje zarówno wiedzę, jak i celowe działanie, w związku z cechami charakterystycznymi czynu zabronionego". Administrator podjął świadomą decyzję, by nie zawiadamiać o naruszeniu Prezesa UODO, jak i osób, których dane dotyczą.
- Stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków Ocena ta dotyczyła reakcji Administratora na pisma Prezesa UODO informujące o obowiązkach ciążących na administratorze w związku z naruszeniem ochrony danych, czy wreszcie wobec wszczęcia postępowania administracyjnego w przedmiocie obowiązku zgłoszenia naruszenia ochrony danych osobowych i zawiadomienia o naruszeniu osób, których dane dotyczą. Administrator ograniczył się wyłącznie do odesłania do poprzednich jego wyjaśnień.
- Kategorie danych osobowych, których dotyczyło naruszenie. Im bardziej szczegółowe czy wręcz wrażliwe dane, tym wyższe ryzyko z naruszeniem związane.

Jednocześnie na wymiar kary nie wpłynęły:

- Działania podjęte przez administratora w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą – Prezes UODO ustalił, że takich działań po prostu nie podjęto.
- Stopień odpowiedzialności administratora z uwzględnieniem środków technicznych i organizacyjnych, jakie wdrożył – naruszenie nie miało związku z takimi środkami bezpieczeństwa.
- Stosowne wcześniejsze naruszenia przepisów RODO - Prezes UODO nie stwierdził wcześniejszych naruszeń.
- Sposób w jaki organ nadzorczy dowiedział się o naruszeniu – Prezes UODO dowiedział się o zdarzeniu od osoby trzeciej, uznano zatem, że administrator nie wyraził żadnej skruchy, co mogłoby wpłynąć na obniżenie kary.

Podsumowując powyższe.

Czy warto zgłaszać naruszenia? Warto! Niewątpliwie warto zgłosić obawy, uwagi czy zastrzeżenia do administratora (np. jako pracownik), aby dać mu, najpewniej we współpracy z IOD, szansę na dokonanie analizy, czy rzeczywiście mamy do czynienia z naruszeniem ochrony danych, a jeśli tak, jakie są jego skutki.

Podejście do tematu przez pryzmat: „lepiej i łatwiej udawać, że nic się nie stało" lub „mam inne obowiązki na głowie" może być bardzo drogim i nieopłacalnym podejściem, a nawet jeśli sytuacji nie uda się uratować i całkowicie odwrócić skutków naruszenia, można je zminimalizować poprzez wykazanie UODO chęci współpracy.

Autor:
Justyna Cybulska
zespół Inspektora Ochrony Danych
adwokat

JUSTYNA JABŁONKA

KANCELARIA WYRZYKOWSCY

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

www.justynajablonka.pl
www. kancelariawyrzykowscy.pl

BLOG dla JST:
https://kancelariawyrzykowscy.pl/pl/blog-jst/
FB:
https://www.facebook.com/kancelariawyrzykowscy