Zmiany w UODO w 4 punktach (15.12.2023 r.)
/ Założenia ogólne /

dr Mirosław Gumularz
radca prawny

1. **Postawienie na edukację, wyjaśnianie i kształtowanie zachowań przy wykorzystaniu "miękkich kompetencji" UODO m.in.:**

    - Materiały, w szczególności poradniki i wyjaśnienia (dopasowane do procesu, sektora i wielkości podmiotów) - pomagające sektorowi publicznemu i prywatnemu osiągnąć zgodność;
    - Wzory i przykłady (np. oceny ryzyka jak brytyjski ICO czy francuski CNIL);
    - Stała komunikacja ryzyk i działań, które są planowane (podobnie jak to robi ENISA);
    - Akcje edukacyjne dla biznesu i osób, których dane są przetwarzane a nie tylko administracji (w tym dla branży IT i nowych technologii);
    - Organizacja dużych wydarzeń (a nie tylko wąsko zakreślonych akcji informacyjnych).

Uwagi szczegółowe

Zgodnie z art. 57 ust. 1 lit. b) RODO organ nadzorczy ma obowiązek rozpowszechniać w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumieniem tych zjawisk, poświęcając przy tym szczególną uwagę działaniom skierowanym do dzieci. UODO jest agregatem ogromnej ilości informacji na temat ryzyk dla ochrony danych (np. rozpatrując skargi, analizując zgłoszone naruszenia ochrony danych, wykonując kontrole), które w sposób ograniczony wykorzystuje w ramach realizacji w/w wymogu wynikającego z RODO. **Dlatego będę chciał wprowadzić rozwiązanie, które nie jest znane w innych państwach członkowskich (na pewno nie w tym zakresie jaki planuję) a może być bardzo dużą pomocą dla stosowania przepisów o ochronie danych osobowych tj. systematyczną publikację wykazów ryzyk (dla określonych procesów przetwarzania danych np. wykorzystanie profilowania). RODO jest oparte na podejściu skupiającym się na eliminowaniu (mitygacji) ryzyk, które dotyczą praw lub wolności osób fizycznych.** Dzięki temu RODO jest adaptowalne do różnych kontekstów przetwarzania danych. Administratorzy (i w niektórych przypadkach także podmioty przetwarzające) mają obowiązek dokonywać ocenę ryzyka. Jednocześnie brakuje wiedzy w tym zakresie. Jest bardzo niewiele praktycznych publikacji w języku polskim wskazujących metody i przykłady scenariuszy, które należy wziąć pod uwagę. Sam jestem redaktorem i współautorem bodaj pierwszej praktycznej publikacji w tym zakresie w Polsce. Administratorzy często bagatelizują wdrażanie wymogów bo nie mają dostatecznej świadomości na temat ryzyk jakie dotyczą wybranych procesów przetwarzania danych zamiast tego skupiają się na elementach formalnych jak wypełnianie upoważnień do przetwarzania danych osobowych. Wskazanymi kwestiami powinien zająć się nowo powołany departament oceny / monitorowania ryzyka dla praw lub wolności o czym będzie mowa niżej.

Wskazana baza wiedzy na temat ryzyk powinna być punktem wyjścia dla wszelkich aktywności urzędu. Pozwoli to skupić się na realnych problemach, w szczególności związanych z wykorzystaniem nowych technologii np. *deepfake,* czy dezinformacja (jeżeli łączy się to z przetwarzaniem danych osobowych). **Nie sposób wytłumaczyć, dlaczego w czasach, gdy inne organy nadzorcze w UE wydają wytyczne dotyczące nowych technologii np. CNIL w zakresie blockchain, cookies, AI, wytyczne dla programistów, polski UODO skupia się na kwestiach pobocznych i czysto formalnych.** Urząd nie może uciekać od tematów trudnych, skomplikowanych i rodzących

kontrowersje (jak problem re-identyfikacji). Co więcej, nawet jeżeli UODO wydaje wyjaśnienia, nie są one aktualizowane np. poradnik dla szkół i placówek oświatowych czy poradnik dla pracodawców nie były aktualizowane od 2018 roku (nie uwzględniają nowych przepisów sektorowych przyjętych w ramach wdrożenia RODO do prawa krajowego). Należy to zmienić, wszelkie wytyczne organu powinny być wydawane i aktualizowane na bieżąco, tak by wspierać administratorów w zapewnianiu zgodności z przepisami.

Aspekt edukacyjny nie może ograniczać się wyłącznie do administratorów i podmiotów przetwarzających. Zgodnie z RODO istotnym zadaniem organu nadzorczego jest upowszechnianie w całym społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem danych oraz rozumienia tych zjawisk (szczególną uwagę poświęcając działaniom skierowanym do dzieci). Jako Prezes UODO zaplanuję organizację szeregu akcji mających na celu zwiększenie świadomości w tym zakresie. Osoby, których dane są przetwarzane muszą wiedzieć jak mogą korzystać z przysługujących im praw, jak postępować gdy ich dane wyciekły, czy wreszcie jak bezpiecznie poruszać się w przestrzeni cyfrowej. **Kluczowe w tym aspekcie będzie także skierowanie akcji edukacyjnych do dzieci i młodzieży, które szczególnie narażone są na takie zjawiska jak cyberbulling czy kradzież danych - jako Prezes UODO będę zabiegał o to by elementy ochrony prywatności były ujęte w programach nauczania**. Chciałbym również by z ramienia UODO powstała platforma edukacyjna, która w sposób dopasowany do wieku będzie przekazywała dzieciom i młodzieży najważniejsze informacje związane z bezpiecznym korzystaniem z sieci i ochroną danych osobowych.

Urząd musi także wprowadzić cykliczne spotkania (online aby zwiększyć ich zasięg) z Inspektorami Ochrony Danych poszczególnych sektorów i branż. Uwzględniając także kwestie wynikające z ustawy o ochronie danych osobowych przetwarzanych w zw. z zapobieganiem i zwalczaniem przestępczości.

2. Otwartość i przewidywalność

- Powołanie Rady Ochrony Danych Osobowych (która powinna być powołana już w maju 2018 r.;
- Otwarcie się na organizacje społeczne i branżowe (wszelkie wytyczne muszą być konsultowane);
- Skoordynowana współpraca z innymi właściwymi podmiotami;
- Jasne komunikowanie jakich działań, dowodów, dokumentów urząd będzie oczekiwał w przypadku różnych typów postępowań (np. w przedmiocie żądań podmiotów danych);
- powrót do uprzednich konsultacji, które obecnie są praktycznie instytucją “martwą”.

Uwagi szczegółowe

Wszelkie materiały muszą być dostosowane nie tylko do danego sektora, lecz także wielkości podmiotu (mikro / mali przedsiębiorcy - średni / duzi etc.). Pozwoli to nie tylko rozpowszechniać wiedzę na temat ochrony danych osobowych w sposób zrozumiały dla danej kategorii odbiorców, **ale także zmniejszyć koszty transakcyjne po stronie tych podmiotów (zwłaszcza małych podmiotów, które często nie mają zasobów na korzystanie z profesjonalnej pomocy przy wdrażaniu środków mających na celu zapewnienie zgodności z przepisami).**

UODO musi w sposób jasny komunikować swoje oczekiwania np. w ramach kontroli sektorowych. Przykładem takiej przewidywalności jest podejście innych organów np. francuskiego, czy irlandzkiego, który zanim rozpoczął weryfikacji zgodności z RODO podmiotów korzystających z mechanizmów cookies w pierwszej kolejności wydał wytyczne i dał czas na ich wdrożenie. Taka postawa - otwartości i dialogu - w mojej ocenie zwiększa zaufanie do organów Państwa i zachęca do przestrzegania przepisów. Jednocześnie będzie budować prestiż UODO.

Prezes UODO musi także transparentnie wyjaśnić w jakim zakresie będzie realizował swoją kompetencję w przypadku regulacji, które dotyczą ochrony prywatności, ale nie są ściśle związane ze stosowaniem RODO. Przykładem jest tu relacja RODO do przepisów implementujących dyrektywę 2002/58 w zakresie kwestii marketingowych. Nie może być tak, że Polska jest jedynym krajem w UE, gdzie od kilkunastu lat toczy się spór w danym zakresie (np. ilości zgód marketingowych), a urząd nie jest w stanie wydać wyraźnych wytycznych jakie zachowania będzie traktował jako naruszenie RODO. Nie buduje to powagi urzędu. Nie zapewnia to również ochrony obywateli przed niechcianym telemarketingiem (problem styku kompetencji kilku organów). A ilość wyskakujących okienek i checkboxów do zaznaczenia przy zwykłych zakupach w internecie staje się udręką dla konsumentów (osób, których dane są przetwarzane). Ta kwestia stanie się jeszcze bardziej istotna w momencie stosowania aktu o usługach cyfrowych, wejścia w życie aktu o danych czy regulacji dotyczących AI. **W tym kontekście należy skoordynować współpracę m.in. Prezesem UOKiK.** Zwłaszcza, że w przepisach konsumenckich pojawiła się konstrukcja umowy, w ramach której treści cyfrowe są dostarczane w zamian za "dostarczenie" danych osobowych. Podobnie Prezes UODO musi ściśle współpracować z Państwową Inspekcją Pracy. Pomimo zadeklarowania współpracy w tym zakresie trudno doszukać się jakichkolwiek efektów.

UODO musi otworzyć się na współpracę z ośrodkami akademickimi, organizacjami społecznymi, czy branżowymi. UODO musi przy tymi jasno komunikować zasady współpracy w tym zakresie. Nie może być tak, że kryteria korzystania z tych, a nie innych merytorycznych doradców są niejasne. **Wszelkie dokumenty wydawane przez UODO (np. wyjaśnienia, poradniki, etc.), których celem jest kształtowanie zachowań administratorów i podmiotów przetwarzających muszą być poddane konsultacjom aby wykluczyć późniejsze uwagi dotyczące braku jasności dokumentu.** Tak robią organy innych państw. Wszelkie uwagi powinny być omawiane, w szczególności, jeżeli nie są brane pod uwagę. Wyjaśnienia i poradniki powinny być możliwie konkretne, bazować na konkretnych case study (tak jak np. opinie EROD), tak by umożliwiać administratorom rozwiązywanie realnych problemów.

Należy w praktyce "uruchomić" nie funkcjonujący dziś mechanizm uprzednich konsultacji (art. 36 ust. 1 RODO). Uprzednie konsultacje w innych krajach są "codziennym" narzędziem wsparcia administratorów w ramach oceny ryzyka i doboru odpowiednich zabezpieczeń. Natomiast w sprawozdaniu rocznym Prezesa UODO za 2022 r. wskazano, że w 2022 r. do UODO wpłynęło 7 wniosków o uprzednie konsultacje. Żaden z nich - jak wskazuje UODO - nie mógł zainicjować postępowania w sprawie uprzednich konsultacji, gdyż wnioski te obarczone były brakami. Moim zdaniem wynika to z braku przejrzystości UODO w tym zakresie. UODO nie zachęca do uprzednich konsultacji - wyjaśnienia w tym zakresie na stronie www uodo są bardzo lakoniczne. Nie ma chociażby wskazówek co do struktury wniosku o uprzednie konsultacje. Na stronie www UODO znajduje się jeden (sic!) przykład w tym zakresie.

Organ musi być apolityczny – należy podejmować szybkie i stanowcze reakcje na działania naruszające odo niezależnie od tego przez kogo są podejmowane. Prestiż organu został nadwyrężony m.in. sprawą dotyczącą KRS, gdzie NSA (III OSK 2991/21) stwierdził np.:

„Wydanie przez organ postanowienia w którym organ administracji państwowej postawił się ponad polskie sądy i wydane przez nie prawomocne orzeczenia, jednoznacznie wskazuje, że prezes UODO sprzeniewierzył się określonemu w art. 35 ust. 1 ustawy o ochronie danych osobowych ślubowaniu, w którego rocie wprost zapisano, iż zobowiązuje się on do dochowania wierności Konstytucji RP oraz strzeżenia prawa ochrony danych osobowych. Takie postępowanie jest bowiem charakterystyczne dla państw autorytarnych i faszystowskich".

Takie działanie nie mogą przemijać bez echa. Nie mogą też się więcej powtórzyć.

Należy również zachęcać do korzystania z mechanizmu certyfikacji (oceny zgodności z zatwierdzonymi kryteriami certyfikacji), który jest jednym z elementów wykazywania zgodności z przepisami RODO. Prezes UODO zatwierdził dopiero 8 grudnia 2023 r. dodatkowe wymogi akredytacji podmiotów certyfikujących - zatem **stosowanie mechanizmu certyfikacji rozpocznie się najpewniej dopiero za kadencji nowego Prezesa Urzędu. Kluczowe będzie zatem promowanie korzystania z tego mechanizmu i wspieranie podmiotów chcących z niego**

skorzystać. Należy również zachęcać zrzeszenia lub inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających do sporządzania kodeksów postępowania by ułatwić skuteczne stosowanie przepisów RODO - aktualnie w kolejce do zatwierdzenia oczekuje kilka kodeksów. Powinny zostać niezwłocznie zatwierdzone. Należy dokonać oceny przyczyn takiego stanu rzeczy m.in. w zakresie monitorowania przestrzegania tych kodeksów.

3. Reorganizacja urzędu

- Postawienie na nowe departamenty i nowy sposób komunikacji: Departament Komunikacji i Jasnego Języka, Departament Monitorowania Nowych Technologii (w tym AI, IoT), Departament Oceny Ryzyka;
- Stworzenie jednostek zamiejscowych (np. Katowice i Trójmiasto);
- Przegląd działania infolinii (jak komunikuje, czy odpowiedzi są jasne i zrozumiałe i spójne)l
- Przegląd opublikowanych na stronie urzędu pytań, odpowiedzi i wytycznych.

Uwagi szczegółowe

Realizacja kompetencji "miękkich" urzędu musi być oparta o tworzenie materiałów zrozumiałych. Każdy materiał UODO powinien być weryfikowany przez językoznawców pod kątem przejrzystości. Przykładowo w sektorze prywatnym coraz częściej organizacje tworzą komórki organizacyjne zajmujące się weryfikacją tworzonych dokumentów (np. regulaminów usług) pod kątem przejrzystości. Musi powstać także Departament Monitorowania Nowych Technologii. Zgodnie ze sprawozdaniem rocznych UODO za 2022 r. obecnie nowymi technologiami w UODO zajmują się tylko 4 osoby. Kwestią monitorowania ryzyk musi zająć się także osobny departament. Natomiast Departament Oceny / Monitorowania Ryzyka będzie systematycznie komunikował nowe zagrożenia, które zostaną "wykryte" w ramach pracy urzędu dostosowane do sektora, rodzaju narzędzi (np. typów aplikacji) a także kategorii osób, których dane są przetwarzane zwłaszcza w kontekście ochrony dzieci i osób szczególnie zagrożonych (np. wytyczne dla rodziców).

Urząd musi komunikować się poprzez media społecznościowe w sposób dostosowany do kategorii odbiorców. Wystarczy przejrzeć media społecznościowe innych organów nadzorczych, aby dostrzec różnice w sposobie komunikacji.

Należy dokonać także weryfikacji jakości pracy infolinii UODO. Z doświadczenia wiem, że bardzo często odpowiedzi są niejednoznaczne i różne osoby odpowiadają w różny sposób. Osoby komunikujące się z urzędem muszą być w stanie powołać się na uzyskane informacje np. w toku kontroli. Przeglądu wymagają także treści umieszczone na stronie internetowej urzędu - powinny być czytelne, zrozumiałe i aktualne (musi uwzględniać zarówno aktualny stan przepisów, jak i orzecznictwa). Przykładowo **nie może być tak, że na stronie www urzędu publikowane są tylko informacje o orzeczeniach korzystnych dla UODO. Bardzo wiele także decyzji np. omawianych w sprawozdaniach rocznych nie jest publikowanych na stronie www urzędu.**

Co więcej, po ostatnich zmianach na stronie internetowej urzędu, część zasobów jest dostępna jedynie jako archiwum (archwium.uodo.gov.pl) - nie jest jasne czy urząd podtrzymuje wyrażone tam poglądy i stanowiska, zresztą podobnie jak rozsyłany "Biuletyn" opatrzony oświadczeniem, że treści w nim zawarte nie są stanowiskiem urzędu. Należy zweryfikować i przesądzić te kwestie, tak by były one czytelne dla administratorów. Wszelkie oświadczenia i wypowiedzi (np. prasowe) powinny być agregowane w jednym miejscu na stronach

www urzędu. Bardzo wiele stanowisk UODO można poznać (np. w zakresie prawa pracy) wyłącznie po dokonaniu zakupu / wykupieniu prenumeraty w komercyjnym wydawnictwie.

4. Zwiększenie efektywności działań UODO

- Podejmowanie błyskawicznych działań w przypadku wystąpienia zagrożeń czy incydentów bezpieczeństwa (w ramach skoordynowanej współpracy z innymi organami administracji publicznej kompetentnych w zakresie cyberbezpieczeństwa);
- Reorganizacja i zwiększenie efektywności pracy istniejących departamentów np. Departamentu skarg;
- Jasne komunikowanie oczekiwań w przypadku kontroli / innych typów postępowań np. czego osoby kontrolujące będą oczekiwać, jakich informacji, co będzie istotne w czasie kontroli, etc.;
- UODO powinien tłumaczyć co najmniej na j. angielski swoje wytyczne, tak aby jednocześnie budować prestiż poza granicami RP (tak jak robi to np. organ hiszpański czy francuski) / podmioty spoza PL muszą mieć świadomość wymogów regulacyjnych na terenie RP;
- Kontrole skupione na kwestiach istotnych (generujących ryzyka) a nie wyłącznie formalnych.

Uwagi szczegółowe

W przypadku ograniczonych zasobów należy rozważyć zmianę modelu kontroli poprzez ograniczenie ilości pracowników UODO, którzy biorą w nich udział, a także ich zakres. Moim zdaniem zwłaszcza kontrole sektorowe powinny być przeprowadzane bardziej sprawnie, chociażby poprzez skupienie się na głównych ryzykach. Urząd powinien korzystać z pomocy biegłych tam gdzie wymagane są wiadomości specjalne. Przyczyni się to do efektywnego i merytorycznego przebiegu kontroli / postępowania w sprawie ewentualnego naruszenia RODO. Urząd musi odejść od myślania, że tylko dokumenty są dowodem na zgodność z przepisami. Rozliczalność nie jest celem samym w sobie, istotą realizacji wymogów RODO jest ochrona praw lub wolności osób fizycznych.

Należy także poprawić efektywność realizacji żądań (wsparcia w tym zakresie) osób, których dane są przetwarzane np. gdy żądają usunięcia danych. Jest to powiązane z poprawą działania infolinii. Osoby, których dane są przetwarzane powinny mieć możliwość (przed złożeniem skargi do Prezesa UODO) konsultacji swojej sprawy poprzez infolinię tak aby możliwie precyzyjnie opisać na czym polega problem w realizacji praw wynikających z RODO. Należy jednocześnie zwiększyć efektywność pracy departamentów właściwych w tym zakresie. Nie może być tak, że czeka się kilka lat na rozpatrzenie skargi (np. Wyrok WSA w Warszawi II SAB/Wa 501/21). **Postępowania powinny być prowadzone szybko i skutecznie. Dlatego należy dokonać przeglądu wewnętrznych zasad rozpatrywania tej kategorii spraw. Należy w możliwie szerokim stopniu wystandaryzować działania UODO. Jednocześnie administratorzy muszą mieć świadomość, że wielokrotne naruszenie zasad realizacji (uzasadnionych) żądań podmiotów danych będzie kończyć się stanowczą reakcją ze strony urzędu.**

Należy także wykorzystywać inne - niż wyłącznie kontrolne - kompetencje. W tym zakresie dobrym przykładem jest działanie UODO, który przeprowadził postępowanie wyjaśniające odnośnie sprawowania funkcji IOD wysyłając zapytanie do kilkudziesięciu podmiotów w tym zakresie. Takie działanie pozwala zwrócić uwagę podmiotom odpowiedzialnym za realizację wymogów na kwestie ochrony danych osobowych jeszcze przed formalnym wszczęciem kontroli. To działanie miało bardzo duży odzew. Problem jednak w tym, że po wielu miesiącach brak w tym zakresie jakichkolwiek wniosków ze strony UODO.

Zwiększeniu efektywności działań ma służyć także (wspomniana w pkt 3) stworzenie jednostek zamiejscowych, tak aby dać możliwość bezpośredniego kontaktu z urzędem także osobom spoza Warszawy.

Należy zwrócić też uwagę, że na ok 12 tys. naruszeń zgłaszanych do UODO najczęściej zgłaszane naruszenia to: nieprawidłowe zaadresowanie korespondencji czy zagubienie korespondencji przez operatora pocztowego. Można postawić tezę, że administratorzy zgłaszają takie typy naruszeń, które UODO może łatwo zweryfikować. W świecie nowych technologii z pewnością nie jest to główny scenariusz incydentów bezpieczeństwa.