SK&S PRIVACY INSIGHT

Kwartalnik o prawie ochrony danych osobowych

SOŁTYSIŃSKI KAWECKI SZLĘZAK

W tym numerze

PAŹDZIERNIK 2022 | NUMER 2

DSA i DMA z perspektywy ochrony danych osobowych

Maciej Jakubowski
Prawnik, radca prawny
maciej.jakubowski@skslegal.pl
+48 882 630 942

Parlament Europejski oraz Rada UE zatwierdziły dwa rozporządzenia mające stanowić filary regulacji w sektorze cyfrowym. Nowe przepisy obejmą takie podmioty jak portale społecznościowe, dostawców usług chmurowych czy wyszukiwarek internetowych. Regulacje będą oddziaływać również na kwestie związane z przetwarzaniem danych osobowych.

Nowe regulacje a RODO

Zarówno akt o usługach cyfrowych (DSA – Digital Services Act), jak i akt o rynkach cyfrowych (DMA – Digital Markets Act) nie narusza przepisów RODO ani innych przepisów Unii dotyczących ochrony danych osobowych i prywatności w zakresie łączności. Przeciwnie, regulacje te mają uzupełniać dotychczasowe akty prawne, przyczyniając się do tworzenia jednolitych standardów ochrony jednostki m.in. w zakresie przejrzystości przetwarzania, profilowania, czy zgód. Zatem podstawowym aktem w zakresie ochrony danych osobowych pozostaje RODO.

DSA – akt o usługach cyfrowych

Akt o usługach cyfrowych reguluje usługi pośrednie świadczone odbiorcom mającym siedzibę lub miejsce zamieszkania w Unii, niezależnie od siedziby dostawców tych usług. Za dostawców usług pośrednich w rozumieniu rozporządzenia należy uznać podmioty świadczące usługi pośrednictwa, usługi hostingowe, czy platformy internetowe. Celem DSA jest przede wszystkim ustalenie nowych reguł działania na linii platforma – człowiek (odbiorca usługi). Dnia 4 października 2022 r. DSA został zatwierdzony przez Radę UE. Ostatnim krokiem będzie publikacja rozporządzenia w Dzienniku Urzędowym Unii Europejskiej. Przepisy zaczną obowiązywać po 15 miesiącach od wejścia w życie.

- **Ograniczenia w reklamie internetowej** - DSA wprowadza ograniczenia w zakresie prezentowania ukierunkowanej reklamy z wykorzystaniem profilowania. Zgodnie z RODO, administrator przy pozyskiwaniu danych osobowych ma obowiązek poinformować o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu. DSA w tej mierze uzupełnia powyższe regulacje, wprowadzając obowiązek prezentowania informacji o głównych parametrach używanych do określenia odbiorcy, któremu prezentowana jest reklama oraz ewentualnie o sposobie zmiany tych parametrów. W wielu przypadkach dane wykorzystywane do określenia odbiorcy stanowią właśnie dane osobowe takie jak wiek, płeć czy zainteresowania. Zasadą będzie zakaz reklamy ukierunkowanej na podstawie profilowania z wykorzystaniem szczególnych kategorii danych osobowych, takich jak orientacja seksualna, przekonania religijne, czy dane o zdrowiu. Co więcej, profilowanie oparte o dane osobowe zwykłych oraz szczególnych kategorii nie będzie mogło być stosowane, gdy dostawca platformy internetowej z wystarczającą pewnością będzie wiedział, że usługobiorca jest osobą niepełnoletnią. Przy czym w tym przypadku nie będzie dopuszczalne gromadzenie dodatkowych danych osobowych, w tym danych o wieku, w celu oceny, czy odbiorca usługi jest faktycznie osoba niepełnoletnią. W motywach do rozporządzenia wskazuje się, że platforma internetowa może być uznana za dostępną dla osób niepełnoletnich, jeżeli warunki korzystania z platformy dopuszczają korzystanie z niej przez osoby niepełnoletnie (np. część mediów społecznościowych), gdy jej usługa jest skierowana lub w przeważającej mierze wykorzystywana przez niepełnoletnich (np. platformy z grami komputerowymi) lub gdy dostawca jest w inny sposób świadomy, że niektórzy odbiorcy jego usługi są niepełnoletni.

- **Dark patterns** - DSA wprowadza również zakaz wykorzystywania manipulacyjnych interfejsów tj. interfejsów, które z uwagi na stosowane kolory, kształty, obrazki itp. mogłoby wprowadzać użytkowników w błąd, służyć do manipulacji lub w inny sposób istotnie zniekształcać lub ograniczać zdolność do podejmowania swobodnych i świadomych decyzji. Dotychczas metody takie często były wykorzystywane przy odbierania zgód, w tym zgód na przetwarzanie danych osobowych lub w ramach akceptacji plików cookies (np. stosowanie „nieintuicyjnych" kolorów).

DMA - Akt o rynkach cyfrowych

Akt o rynkach cyfrowych ma znacznie węższe zastosowanie, gdyż jest adresowany do największych podmiotów na rynku usług cyfrowych tzw. strażników dostępu (ang. Gatekeepers). O przyznaniu statusu strażnika dostępu będzie decydowała Komisja Europejska po uprzedniej notyfikacji przez podmiot, który osiągnął progi wskazane w rozporządzeniu. Głównym celem przepisów jest wyznaczenie reguł działania na linii wielkie platformy – biznes (w tym mniejsze podmioty funkcjonujące na rynku cyfrowym), w szczególności przez zwiększenie konkurencyjności. Publikacja rozporządzenia w Dzienniku Urzędowym Unii Europejskiej planowana jest na 13 października 2022 r. Przepisy zaczną obowiązywać po 6 miesiącach od wejścia w życie.

- **Zakaz łączenia danych** - Rozporządzenie wprowadza generalny zakaz łączenia danych osobowych z różnych źródeł bez prawidłowo udzielonej zgody użytkownika. Ma to zmniejszyć przewagę największych platform w stosunku do pozostałych podmiotów na rynku usług cyfrowych. Zgodnie z art. 5 DMA strażnikom dostępu zabrania się:

  1. przetwarzania w celu świadczenia usług reklamy internetowej danych osobowych użytkowników korzystających z usług podmiotów trzecich, które korzystają z usług platformy głównej;

  2. łączenia danych osobowych pochodzących z różnych platform zarządzanych przez danego strażnika dostępu lub z danymi osobowymi pochodzącymi z usług podmiotów trzecich;

  3. wzajemnego wykorzystywania danych osobowych użytkowników z różnych platform zarządzanych przez danego strażnika dostępu;

  4. rejestrowania użytkowników do innych usług świadczonych przez strażnika dostępu w celu łączenia danych osobowych;

W przypadku odmowy lub wycofania zgody na reklamy internetowe, strażnik dostępu nie będzie miał możliwości powtórnej prośby o zgodę w tym samym celu więcej niż raz w okresie jednego roku. Jednocześnie w takiej sytuacji brak wyrażenia zgody nie powinien pociągać za sobą ograniczeń w podstawowych funkcjonalnościach platformy.

- **Obowiązek raportowania w zakresie metod profilowania** - DSM kładzie duży nacisk na transparentność działania strażników dostępu. Przejawem tego będzie obowiązek poddania niezależnemu audytowi opisu podstaw, na których odbywa się profilowanie konsumentów. Badane będzie czy do profilowania są wykorzystywane dane osobowe, cel, dla którego profil jest przygotowywany i ostatecznie wykorzystywany, czas trwania profilowania, wpływ takiego profilowania na usługi strażników dostępu oraz kroki podjęte w celu skutecznego umożliwienia użytkownikom końcowym uświadomienia sobie stosowania takiego profilowania, a także działań zmierzających do uzyskania ich zgody lub zapewnienia możliwości odmowy lub cofnięcia zgody. Tak sporządzony raport będzie przekazywany do Komisji Europejskiej.

Podsumowanie

Rozporządzenia DSA oraz DMA stanowią ważny krok w kierunku uregulowania w Unii usług cyfrowych. Kluczowym elementem z perspektywy ochrony danych osobowych jest kompatybilność nowych przepisów z dotychczasowymi regulacjami, co powinno przełożyć się na tworzenie spójnego systemu ochrony jednostki w wirtualnym świecie.

Transfery danych poza EOG – aktualny stan prawny

Katarzyna Klonecka
Prawnik, adwokat
katarzyna.klonecka
@skslegal.pl
+48 602 151 178

Od czasu wydania wyroku Trybunału Sprawiedliwości Unii Europejskiej znanego także jako wyrok ws. „Schrems II" (nasz alert na ten temat dostępny jest tutaj), kwestia transferów danych osobowych poza EOG – w szczególności do Stanów Zjednoczonych – nadal budzi dużo kontrowersji. Poniżej wskazujemy najważniejsze kwestie, które firmy powinny uwzględnić rozważając przekazywanie danych poza EOG.

Praktyczne znaczenie transferów dla działalności biznesowej

Zmieniający się stan prawny dot. transferów danych poza EOG wiąże się z wieloma wyzwaniami dla administratorów danych, w szczególności **w kontekście używania rozwiązań międzynarodowych dostawców** (np. korzystania z technologii reklamowej – adtech i korzystania z innych rozwiązań takich dostawców jak Facebook lub Google). Regulacje dotyczące transferów pokrywają zarówno sytuacje gdy dane trafiają docelowo do państwa trzeciego i tam są przechowywane (*data at rest*), jak i sytuacje gdy dane są przesyłane przez kraj spoza EOG (*data in transit*), a także gdy dostęp do danych znajdujących się w Unii jest wyłącznie uzyskiwany spoza EOG. Jak widać, **pojęcie transferu jest bardzo szerokie i może obejmować wiele sytuacji związanych z codziennym funkcjonowaniem biznesu, a potencjalnie mogą nawet wymusić zmianę dotychczasowych procesów.**

Konsekwencje Schrems II na poziomie unijnym – nowe klauzule i rekomendacje

Wyrok *Schrems* II nie tylko unieważnił Privacy Shield (podstawę transferów do Stanów Zjednoczonych niewymagającą żadnych dodatkowych kroków po stronie administratorów), ale i wskazał dodatkowe wymogi związane z transferami. Przede wszystkim z wyroku wynika, że **samo oparcie się na wydanych przez Komisję Europejską standardowych klauzulach umownych może okazać się niewystarczające.** Zgodnie z ww. wyrokiem, **należy każdorazowo ocenić skuteczność tych klauzul w świetle uwarunkowań prawnych państwa spoza EOG oraz, w razie potrzeby, wdrożyć dodatkowe zabezpieczenia danych.** Standardowe klauzule umowne są bowiem jedynie kontraktem, który nie zawsze może okazać się skuteczny w świetle mających zastosowanie przepisów prawa.

Wskutek powyższego, **Europejska Rada Ochrony Danych wydała zalecenia dotyczące wdrażania dodatkowych – towarzyszących standardowym klauzulom umownym – zabezpieczeń zapewniających skuteczność ochrony danych osobowych podczas transferu**, w szczególności w świetle ustawodawstwa umożliwiającego władzom państw trzecich dostęp do danych. Zalecenia wskazują przykładowe środki, które mogą uzupełniać standardowe klauzule umowne, w tym środki organizacyjne i techniczne oraz dodatkowe środki umowne. Celem wdrażania tych środków jest zapewnienie merytorycznej równoważności ochrony transferowanych danych z ochroną przysługującą w Unii. Administratorzy mogą korzystać z tych wytycznych by prawidłowo uzupełnić używane przez siebie standardowe klauzule umowne.

Ponadto, **Komisja Europejska przyjęła nowe standardowe klauzule umowne**, które stanowią obecnie jeden z dozwolonych przez RODO mechanizmów transferów danych poza EOG. To na nich powinni bazować administratorzy, jeżeli chcą wszcząć nowe transfery i nie zidentyfikowali innej podstawy dla ich wykonania (np. decyzji o adekwatności).

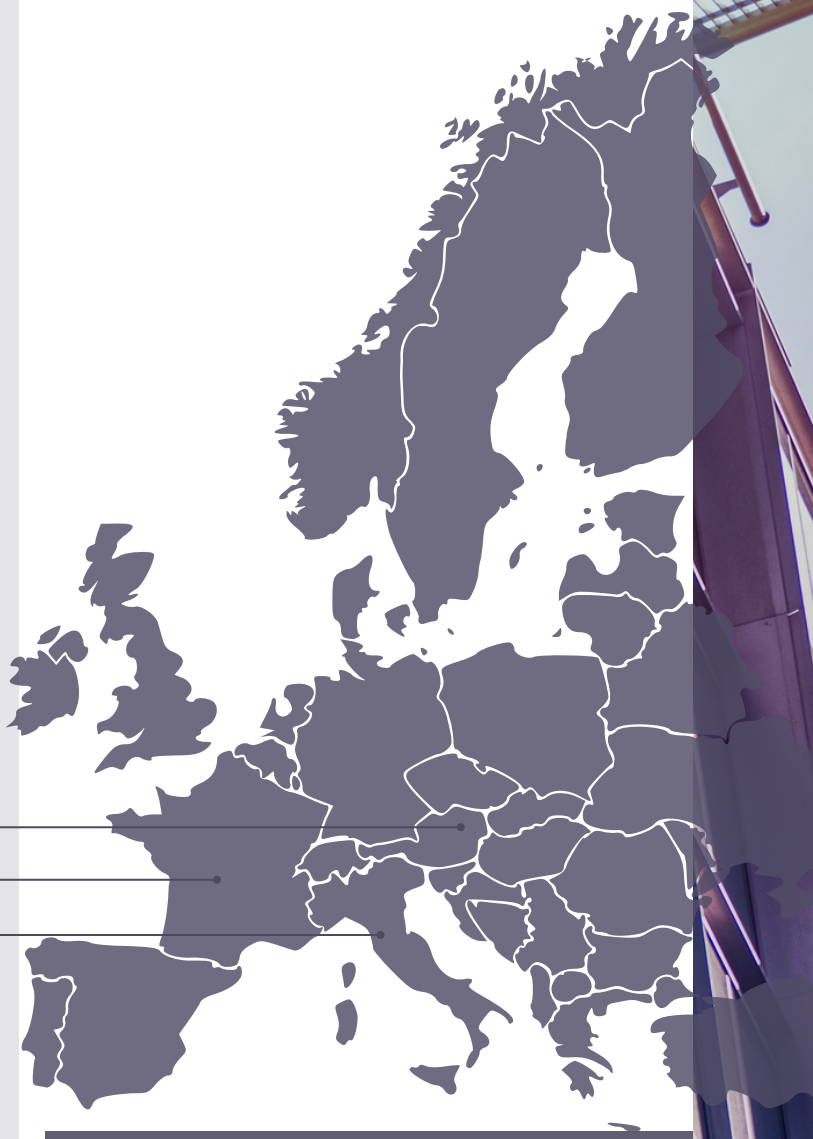
W przypadku transferów głównym problemem może się okazać to, że przepisy państwa trzeciego pozwalające na dostęp jego władz do danych zapewniają zbyt szeroki i niepodlegający kontroli dostęp do danych Europejczyków, którego nie blokują standardowe klauzule umowne. Takie regulacje były czynnikiem determinującym unieważnienie Privacy Shield oraz są wykorzystywane do podważania możliwości wysyłania danych do Stanów Zjednoczonych w decyzjach organów nadzorczych i TSUE.

Decyzje organów nadzorczych i praktyki innych organów państwowych

Prezes Urzędu Ochrony Danych Osobowych nie wydał do tej pory własnych wytycznych związanych z transferami danych, ale powołuje się na działania na poziomie unijnym. Możemy jednak spodziewać się ujawnienia własnego stanowiska PUODO na temat transferów, bowiem do polski trafiło 5 ze 101 skarg wniesionych na administratorów korzystających z rozwiązań Facebooka i Google, dokonujących m.in. transferów danych do USA (skargi te wniosła fundacja NYOB po wyroku ws. *Schrems II*).

Mimo że w Polsce nie podano jeszcze informacji o postępowaniach toczących się wskutek tych skarg, organy nadzorcze w innych państwach unijnych wydały już decyzje w niektórych sprawach. **Część organów nadzorczych (Hiszpania, Luksemburg) odrzuciło skargi ze względu na to że administratorzy przestali korzystać ze wskazanych w skardze narzędzi.** Co ciekawe, jak wynika z informacji pozyskanych od NYOB, okoliczność ta nie zadecydowała o odrzuceniu skarg we wszystkich jurysdykcjach.

Decyzje >>



Niektóre organy nadzorcze (Austria, Francja, Włochy) wskazywały, że korzystając z narzędzi Google dokonujących transferów do Stanów Zjednoczonych administratorzy dopuszczali się naruszenia RODO, ponieważ – mimo zawartych standardowych klauzul umownych – amerykańskie służby wywiadowcze miały szerokie prawa nadzorcze wobec dostawców narzędzi i nie doszło do zapewnienia odpowiedniej ochrony za pomocą ww. klauzul.

Podejmowane są również inne działania na poziomie lokalnym np. w Danii, zakazano korzystania z rozwiązań Google w szkołach.

Powyższe decyzje będą prawdopodobnie służyły jako wytyczne również przy ocenie transferów do innych państw trzecich nie zapewniających takiej samej ochrony jak EOG.

UWAGA!

W przypadku w którym dotychczas wykonywane transfery danych osobowych poza EOG wykonywane były na podstawie poprzednio obowiązujących standardowych klauzul umownych, konieczna jest ich aktualizacja. Od 27 grudnia 2022 r. jedynie standardowe klauzule umowne z czerwca 2021 r. mogą być stosowane!

Co powinni robić administratorzy chcący dokonać transferu danych?

Przede wszystkim należy pamiętać, że w przypadku państw spoza EOG, w stosunku do których została wydana decyzja o adekwatności, uwagi wskazane w niniejszym artykule nie mają zastosowania. Decyzja ta stanowi samoistną podstawę transferów i nie jest konieczne dodawanie dodatkowych środków zabezpieczających.

Lista państw, w stosunku do których została wydana taka decyzja

W przypadku opierania transferów na innych podstawach wskazanych w art. 46 RODO należy:

- zidentyfikować operacje transferów danych poza EOG;
- ocenić, czy istnieją przepisy lub praktyki obowiązujące w odpowiednim państwie spoza EOG, które mogą mieć wpływ na skuteczność stosowanej podstawy transferu i zabezpieczeń;
- ustalić i wdrożyć ewentualne środki uzupełniające, tak aby stopień ochrony przekazywanych danych był merytorycznie równoważny temu wynikającemu z prawa unijnego;
- dokonywać, w odpowiednich odstępach czasu, ponownej oceny stosowanych środków i mającego zastosowanie stanu prawnego.

W celu wykonania powyższych kroków zazwyczaj wdrażane są Transfer Impact Assessments („TIA"). TIA to analiza wpływu i skutków dla bezpieczeństwa transferu danych osobowych do kraju spoza EOG, wobec którego nie wydano decyzji o adekwatności. Służy ona spełnieniu wymogów RODO dotyczących rozliczalności. Należy wskazać, że analiza taka jest również wymagana przez zapisy standardowych klauzul umownych.

Wszędzie gorzej gdzie nas nie ma?

Koncentrowanie się na transferach do państw trzecich powoduje często, że mniejszą uwagę przykłada się do dostępu do danych przez organy porządku publicznego w samej Unii Europejskiej. Warto podkreślić, że tutaj również często pojawiają się kontrowersje związane z dostępem podmiotów trzecich (w tym służb państwowych) do informacji o obywatelach. Tytułem przykładu, Fundacja Panoptykon, działająca na rzecz prywatności, **wielokrotnie zwracała uwagę** na to że w Polsce służby mają możliwość inwigilacji bez odpowiedniej kontroli, **a sprawy tego dotyczące docierają przed ETPCz**. Tym samym, przyjęty w dotychczasowych wytycznych i decyzjach model w którym istnieje założenie, że transfery poza EOG są ryzykowne (niektóre wręcz zakazane) i ich wykonywanie wymaga wielu dodatkowych kroków, a dane w EOG są bezpieczne tworzy wrażenie ochrony pozostającej w dużej mierze na poziomie teoretycznym.

CIEKAWOSTKI

Wysokie kary i zakaz prowadzenia działalności za zautomatyzowane rozpoznawanie obywateli za pomocą biometrii i informacji pobranych z Internetu

Organy ds. danych osobowy wielu krajach, w tym w **Grecji**, **Włoszech** i **Francji** wydały decyzje dot. naruszeń prawa ochrony danych osobowych przez Clearview AI, w tym nałożyły na ww. firmę znaczące kary finansowe (np. 20 mln EUR w Grecji i Włoszech oraz 7,5 mln GBP w Wielkiej Brytanii). Organy nadzorcze wydawały także nakazy zaprzestania działalności oraz usunięcia baz danych.

Praktyki Clearview AI polegały na zbieraniu wizerunków z mediów społecznościowych i innych publicznych źródeł w sposób zautomatyzowany (web scrapping). Mechanizm zapisywał wszelkie obrazy zidentyfikowane jako wizerunek człowieka, wraz z informacjami o pliku (np. link do strony źródłowej, informacje o miejscu zrobienia zdjęcia). Dane te były następnie identyfikowane przez algorytm i dopasowywane do innych zdjęć w bazie firmy. Dostęp do bazy był następnie sprzedawany firmom prywatnym oraz organom ścigania lub służbom specjalnym. Podmioty te, po wgraniu do niego konkretnego zdjęcia, mogły zidentyfikować konkretną osobę i pozyskać inne informacje zebrane o niej w bazie Clearview AI (listę wszystkich zebranych zdjęć wraz z linkami do konkretnych stron i danych zebranych w toku web scrapingu). Tym samym, dochodziło do przetwarzania danych osobowych, w tym danych biometrycznych (przetwarzanie zdjęć uznaje się za przetwarzanie danych biometrycznych jeżeli są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości – wynika to wprost z motywu 51 RODO).

Należy podkreślić, że mimo stworzenia rozbudowanego systemu przez spółkę, musi się ona obecnie mierzyć z zakazem prowadzenia planowanej działalności w wielu krajach. Pokazuje to jak istotne jest praktyczne zastosowanie koncepcji privacy by design.

Powyżej opisane działania organów wpisują się w szeroką dyskusje dot. zasad stosowania mechanizmów rozpoznawania twarzy. Na poziomie unijnym pojawiają się głosy o zakazaniu używania kamer posługujących się sztuczną inteligencją do skanowania i identyfikacji twarzy ludzi w przestrzeni publicznej, a – jak donosi portal POLITICO - **zwolennicy takiego podejścia tworzą rosnącą grupę w Parlamencie Europejskim** . Z drugiej strony, z takich rozwiązań chcieliby korzystać pracodawcy w przypadku dostępu do szczególnie krytycznych informacji czy organizatorzy imprez masowych w celu zapewnienia bezpieczeństwa. Pogodzenie tych interesów może być trudne bez dodatkowych regulacji prawnych lub wytycznych, dlatego warto obserwować prace i dyskusje nad takimi regulacjami toczące się obecnie w strukturach unijnych.

Kolejne kary za nienależytą ochronę danych osobowych sygnalistów

Nienależyta ochrona danych osobowych sygnalistów była przyczyną nałożenia przez włoski organ nadzorczy GPDP (Garante Per La Protezione Dei Date Personali) kolejnej kary pieniężnej. Decyzją z 4 kwietnia 2022 r. GPDP nałożył na administratora danych – Szpital Publiczny w Perugii oraz podmiot przetwarzający – ISWEB S.p.A. dostawcę systemu do obsługi zgłoszeń sygnalistów kary pieniężne – w obu przypadkach – w wysokości 40.000 EUR.

Zgodnie z ustaleniami GPDP, dostęp do aplikacji internetowej służącej do zgłaszania nieprawidłowości, opartej na oprogramowaniu open source, dostarczanej przez ISWEB S.p.A., był możliwy za pośrednictwem systemów, które, nie będąc odpowiednio skonfigurowane, rejestrowały i przechowywały dane dotyczące przeglądania stron przez użytkowników, co pozwalało na identyfikację osób korzystających z tej aplikacji, w tym potencjalnych sygnalistów. Ponadto, pracownikom nie przekazano żadnych informacji na temat przetwarzania ich danych osobowych w celu zgłaszania nieprawidłowości, nie przeprowadzono oceny skutków dla ochrony danych (DPIA); jak również w rejestrze czynności przetwarzania nie został uwzględniony ten proces. W ocenie włoskiego organu nadzorczego administrator danych nie ustanowił odpowiednich środków technicznych i organizacyjnych w celu zapewnienia właściwego poziomu bezpieczeństwa, uwzględniając szczególne ryzyko wynikające z takiego przetwarzania, co wymagało wdrożenia systemu zarządzania zgłaszaniem nieprawidłowości zgodnego z zasadami „Privacy by design" oraz „Privacy by default".

W odniesieniu do podmiotu przetwarzającego włoski organ nadzorczy stwierdził naruszenie w przedmiocienieuregulowania przez ISWEB S.p.A. stosunków z dostawcą usług hostingowych (brak umowy powierzenia przetwarzania danych) zarówno w przypadku działania w charakterze podmiotu przetwarzającego (na rzecz Szpitala Publicznego), jak i w przypadku działania w charakterze odrębnego administratora danych (w odniesieniu do swoich usług wewnętrznych, np. dotyczących zarządzania pracownikami lub działań księgowych i administracyjnych).

Decyzja GPDP w odniesieniu do administratora danych

Decyzja GPDP w odniesieniu do podmiotu przetwarzającego

Szeroka interpretacja szczególnych kategorii danych osobowych wg. TSUE

W dniu 1 sierpnia 2022 r. Trybunał Sprawiedliwości wydał orzeczenie (w sprawie C-184/20), w którym wypowiedział się m.in. co do zakresu szczególnych kategorii danych osobowych, o których mowa w art. 9 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) „RODO".

Sprawa jest pokłosiem wniosku litewskiej Głównej Komisji Etycznej (organu odpowiedzialnego za zwalczanie korupcji) się do jednego z dyrektorów instytucji publicznej o złożenie oświadczenia o tzw. interesach prywatnych. W zakres tego oświadczenia wchodzą m.in. następujące informacje: (i) imię, nazwisko, numer identyfikacji osoby fizycznej, numer ubezpieczenia społecznego, (ii) określenie osoby prawnej, której członkiem lub wspólnikiem jest składający oświadczenie lub jego współmałżonek, konkubent lub partner, (iii) wskazanie bliskich lub innych znanych składającemu oświadczenie osób lub danych, z którymi relacja mogłaby powodować konflikt interesów. Część z powyższych informacji podlega publikacji na stronie internetowej Głównej Komisji Etycznej. Dyrektor instytucji publicznej wniósł sprawę do litewskiego sądu, który z kolei powziął wątpliwość w zakresie zgodności przepisów antykorupcyjnych na Litwie a RODO, w tym m.in. w zakresie art. 9 ust. 1 RODO.

Trybunał Sprawiedliwości w tej sprawie wskazał że art. 9 RODO: ***należy interpretować w ten sposób, że zamieszczanie, na stronie internetowej organu publicznego odpowiedzialnego za gromadzenie oświadczeń o interesach prywatnych i kontrolę ich treści, danych osobowych mogących pośrednio ujawnić orientację seksualną osoby fizycznej, stanowi przetwarzanie dotyczące szczególnych kategorii danych osobowych w rozumieniu tych przepisów.***

Trybunał Sprawiedliwości uznał, że:

- sama informacja o imieniu małżonka czy też konkubenta lub partnera osoby składającej oświadczenie o tzw. interesach prawnych może udzielić pewnych informacji dotyczących życia lub orientacji seksualnej nie tylko składającego oświadczenie, ale również współmałżonka, konkubenta lub partnera osoby składającej oświadczenie (motyw 119 wyroku);
- w zakres art. 9 ust. 1. RODO powinny wchodzić dane, które poprzez intelektualną operację kojarzenia lub dedukcji wskazują na orientację seksualną osoby fizycznej (motyw 120 wyroku);
- szeroka wykładnia art. 9 ust. 1 RODO jest zgodna z celem RODO, jakim jest zagwarantowanie wysokiego poziomu ochrony podstawowych praw i wolności osób fizycznych, a zwłaszcza ich życia prywatnego, w zakresie przetwarzania danych osobowych, które ich dotyczą (motyw 125 wyroku).

Wyrok Trybunału Sprawiedliwości z całą pewnością zaostrza obowiązki spoczywające na administratorach. Wymaga on od administratorów głębszego przemyślenia czy poszczególne dane osobowe mogą służyć w drodze skojarzenia do ujawnienia szczególnych kategorii danych osobowych.

Sylwia Macura-Targosz
Starszy Prawnik, radca prawny
sylwia.macura-targosz@skslegal.pl
+48 694 415 447

Adrianna Gnatowska
Prawnik, adwokat
adrianna.gnatowska@skslegal.pl
+48 538 628 072

ORZECZNICTWO & DECYZJE

Kolejne orzeczenie dot. przetwarzania danych w rekrutacji

Wojewódzki Sąd Administracyjny w Warszawie uznał że pracodawca ma prawo przetwarzać dane kandydatów do pracy po zakończonej rekrutacji w celu obrony przed ewentualnymi roszczeniami z tytułu dyskryminacji – wyrok z 4 sierpnia 2022 r. (sygn. akt. II SA/Wa 542/22). Sąd stwierdził, że:

- Administrator danych ma interes prawny, w rozumieniu przepisów RODO (art. 6 ust. 1 (f) RODO), do przetwarzania (wyłącznie poprzez ich przechowywanie) danych osobowych kandydata do pracy w celu obrony przed roszczeniami tak kandydata do pracy, jak i innych osób, które uczestniczyły w procesie rekrutacji, a które mogą być skutecznie dochodzone przez okres przedawnienia roszczeń ze stosunku pracy wynikający z art. 291 k.p., tj. przez okres 3 lat od dnia, w którym roszczenie stało się wymagalne.

- Interes prawny administratora danych w postaci przechowywania danych uczestnika postępowania rekrutacyjnego przez znany, z góry określony okres (okres przedawnienia roszczeń pracowniczych wynikający z art. 291 k.p.) z potencjalną możliwością wykorzystania ich w postępowaniu nie narusza ani nie wpływa negatywnie na sytuację prawną uczestników postępowania rekrutacyjnego.

- Przesłanka prawnie uzasadnionego interesu, o której mowa w art. 6 ust. 1 (f) RODO, może dotyczyć sytuacji jeszcze nie istniejącej, tj. celem wynikającym z prawnie uzasadnionych interesów realizowanych przez administratora może być konieczność udowodnienia potrzeby dochodzenia lub obrony przed roszczeniem ewentualnym, jeszcze nie istniejącym. Takie przetwarzanie nie ma charakteru przetwarzania „na zapas".

Przypomnijmy stanowisko PUODO w tym przedmiocie (prezentowane od 2018 r.)

Co do zasady pracodawca powinien trwale usunąć dane osobowe kandydata, z którym nie zdecydował się zawrzeć umowy o pracę, niezwłocznie po zakończeniu procesu rekrutacji, tj. po podpisaniu umowy o pracę z nowozatrudnionym pracownikiem, chyba że ziściły się inne przesłanki uprawniające administratora do ich przetwarzania. Wydłużenie okresu przechowywania danych zawartych w aplikacji powinno być zatem wyjątkiem od reguły niezwłocznego ich usuwania oraz powinno być szczególnie uzasadnione. W ocenie organu niedopuszczalne jest przetwarzanie danych osobowych niejako "na zapas" z założeniem, że mogą być one ewentualnie przydatne w przyszłości oraz z odwołaniem się przy tym do przepisów dotyczących przedawnienia roszczeń cywilnoprawnych.

Wyrok Wojewódzkiego Sądu Administracyjnego idzie w dobrym kierunku. Jeśli wyrok stanie się prawomocny, pracodawcy będę mieli realne szanse obrony przed ewentualnymi roszczeniami osób niezatrudnionych, jak również będą w stanie lepiej realizować obowiązek przeciwdziałania dyskryminacji w zatrudnieniu.

WSA utrzymuje karę nałożoną przez PUODO na Bank Millenium S.A.

Wojewódzki Sąd Administracyjny w wyroku z 1 lipca 2022 r. rozpatrując skargę Banku Millenium S.A. na decyzję PUODO (II SA/WA 4143/21) oddalił skargę banku i utrzymał decyzję organu nakładającą na administratora karę w wysokości 363.832 PLN. Wyrok jest nieprawomocny.

Działaniami, które doprowadziły do nałożenia przez PUODO kary w zaskarżonej decyzji było stwierdzenie naruszenia ochrony danych polegającego na zgubieniu przesyłki z dokumentacją bankową klienta przez firmę kurierską przy jednoczesnym braku zgłoszenia niniejszego naruszenia przez administratora.

Organ w zaskarżonej decyzji krytycznie ocenił działania podjęte przez administratora w związku z naruszeniem wskazując, w szczególności że:

- brak zgłoszenia naruszenia do PUODO należy uznać za zupełnie nieuzasadniony w niniejszym stanie faktycznym, szczególnie biorąc pod uwagę, że:
  1. przeprowadzona przez bank w oparciu o metodologie ENISA wewnętrzna ocena ryzyka wskazała na średni poziom ryzyka naruszenia praw i wolności osób fizycznych,
  2. Dane utracone w wyniku zdarzenia obejmowały dane objęte tajemnicą bankową, w tym numery rachunków i PESEL klienta,

- zaniechania banku w związku z niniejszym naruszeniem wskazują na wysoki poziom winy administratora, co potwierdza sam sposób realizacji obowiązków administratora po wykryciu naruszenia, którego sposób realizacji uniemożliwiał osobie której dane zostały zagubione realizację swoich praw (np.: poprzez zgłoszenie alertu BIK).

Jednocześnie organ w całości zakwestionował argumentację Sądu opartą o tezę, iż to firma kurierska była administratorem danych zawartych w zagubionej dokumentacji, więc to ona powinna dokonać zgłoszenia do PUODO.

Wojewódzki Sąd Administracyjny w całości zgodził się z argumentacją PUODO. Sąd podkreślił, że :

- Ocena ryzyka naruszenia praw i wolności osoby, której dane zostały utracone powinna być dokonywana z perspektywy tej osoby, a brak precyzyjnego zawiadomienia osoby, spełniającego wymogi z art. 34 ust. 2 RODO uniemożliwia realizację tych praw. Prawidłowe zawiadomienie powinno zawierać precyzyjne i opisowe przedstawienie dostępnych uprawnionemu praw i jest wykonywane w celu minimalizacji skutków naruszenia.

- Z racji tego, że treść utraconych dokumentów objęta była tajemnicą bankową, oczywistym jest, że administratorem danych widniejących na nich jest Bank, będący nadawcą przesyłki. Bank samodzielnie w tym zakresie określa cele i sposoby przetwarzania, w przeciwieństwie do informacji zawartych na oznaczeniu przesyłki, których administratorem (wyłącznie w zakresie niezbędnym do dostarczenia przesyłki) może być też niezależnie operator pocztowy.

- Do oceny ryzyka naruszenia praw i wolności osób fizycznych kluczowa jest ocena ryzyka utraty kontroli nad danymi przez administratora, a nie wyłącznie ocena zapoznania lub wykorzystania danych.

Wyrok jest istotny również dla operatorów pocztowych, gdyż przesądza ze nie są oni generalnie administratorami danych zawartych w przesyłce (co do której zawartości często nie mają nawet wiedzy), ani podmiotami przetwarzającymi takie dane. Są oni natomiast administratorami danych zawartych na przesyłce tj. dane nadawcy czy odbiorcy, które są niezbędne do wykonania usługi.

Monitoring nadal z problemami

W ostatnich miesiącach pojawiło się kilka ciekawych rozstrzygnięć wydanych przez europejskie organy nadzorcze oraz sądy w zakresie naruszeń związanych z przetwarzaniem danych osobowych w związku z prowadzonym monitoringiem.

- W wyroku wydanym w Irlandii (sprawa *Doolin v The Data Protection Commissioner [2022]* IECA 117), Sąd ustalił, że w zakładzie pracy został wdrożony monitoring CCTV służący zapewnieniu bezpieczeństwa i ochrony zdrowia w miejscu pracy. Pracownicy zostali poinformowani przez pracodawcę o wyżej wymienionych celach przetwarzania. Pracodawca prowadząc postępowanie wyjaśniające w sprawie incydentu mającego miejsce w zakładzie pracy, zapoznał się z nagraniami obrazu CCTV z pracowniczej stołówki. Następnie pracodawca wykorzystał te nagrania obrazu z monitoringu CCTV w celu przeprowadzenia postępowania dyscyplinarnego przeciwko pozwanemu. Zdaniem pozwanego taki cel wykorzystania nagrań obrazu nie mieścił się w celach, dla których prowadzony był monitoring. Ostatecznie sąd zgodził się z pracownikiem i stwierdził, że przetwarzanie dla celów postępowania dyscyplinarnego nie było zgodne z prawem i stanowiło zatem naruszenie zasady ograniczenia celu, zgodnie z art. 5.1.b. RODO.

- W Luksemburgu **organ nadzorczy** („CNPD") przeprowadzając kontrolę u jednego z administratorów, ustalił że administrator ten nie uregulował w wewnętrznej dokumentacji zasad przetwarzania danych osobowych pracowników w związku z prowadzonym monitoringiem CCTV. Dodatkowo administrator nie potrafił wykazać dlaczego prowadzenie monitoringu CCTV jest konieczne. Administrator wyjaśniał, że poinformował swoich pracowników ustnie o prowadzonym monitoringu CCTV, co CNPD uznał za niewystarczające. Dodatkowo, monitoring CCTV sprawował stały nadzór nad pracownikami na ich stanowiskach pracy, a także obejmował teren sąsiadujących nieruchomości. W ten sposób monitoring CCTV nie zapewniał prywatności pracowników oraz wykraczał poza zasadę ograniczenia celu, zgodnie z art. 5.1.c. RODO. CNPD ustalił również, że osoby trzecie także nie zostały poinformowane o monitoringu wizyjnym. Administrator prowadził również monitoring GPS samochodów wynajmowanych swoim klientom. O monitoringu GPS tych samochodów klient dowiadywał się jedynie z treści umowy, co również CNPD uznał za niewystarczające. Informacja o obecności urządzeń geolokalizacyjnych nie była również przekazywana pracownikom. W konsekwencji CNPD nałożył na administratora karę w wysokości prawie 5 tys. EUR.

- W Polsce **PUODO** w sprawie dotyczącej Stołecznego Ośrodka dla Osób Nietrzeźwych stwierdził naruszenie przepisów RODO, tj. art. 6.1. w zw. z art. 5.1.a. RODO. Naruszenie polegało na przetwarzaniu danych osobowych bez podstawy prawnej, tj. nagrywania i utrwalania dźwięku (głosu) za pośrednictwem systemu monitoringu prowadzonego u administratora. Administrator wskazał, że celem takiego przetwarzania danych osobowych jest m.in. sprawowanie stałego nadzoru osób dla zapewnienia bezpieczeństwa. Utrwalony dźwięk (głos) administrator przetwarzana przez okres 30-60 dni (lub dłużej gdy nagranie ma być zabezpieczone dla celów postępowań). Natomiast, za podstawę prawną takiego przetwarzania administrator wskazał art. 6.1.c. RODO, w tym powołał się na ustawę o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, aktach wykonawczych do tej ustawy oraz statucie placówki. PUODO w swojej decyzji wskazał, że utrwalanie dźwięku (głosu) w ramach monitoringu wideo należy uznać za nadmiarowe i niecelowe, a w konsekwencji nie wynika z przepisów RODO oraz ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi.

Wyżej opisane sprawy potwierdzają, że niezależnie od kraju w którym działa, administrator musi poinformować o wszelkich celach monitoringu, a informacja o monitoringu powinna być udokumentowana. Dodatkowo, prowadzany monitoring nie może być nadmiernie szeroki.

Informacje zapisane w plikach cookies nie zawsze stanowią dane osobowe

Wojewódzki Sąd Administracyjny Warszawie w dniu 11 lipca 2022 r. (sygn. akt II SA/Wa 3993/21) uchylił decyzję PUODO, w której organ nałożył upomnienie na spółkę iSecure sp. z o.o., zarzucając jej m.in. udostępnienie podmiotom trzecim danych osobowych użytkownika (pozyskanych przez cookies zainstalowane na jego komputerze) bez podstawy prawnej (wyrok nie jest prawomocny). Sąd uznał że:

- PUODO nie wyjaśnił na jakiej podstawie ustalił, że istnieje uzasadnione prawdopodobieństwo zidentyfikowania użytkownika w powiązaniu z adresem IP oraz ID plików cookies – przytoczony przez PUODO wyrok NSA (z 19 maja 2011 r. sygn. akt I OSK 1079/10) wyraźnie wskazuje, że adresy IP nie zawsze mogą być traktowane jako dane osobowe; co więcej, w wyroku tym wskazane zostały warunki kwalifikacji adresu IP jako danej osobowej, jednak PUODO nie wyjaśnił, czy w tej sprawie zostały one spełnione. Organ nadzorczy niejako „z góry" założył, że zarówno adres IP jak i ID plików cookies są danymi osobowymi.

- Przepisy RODO nie rozstrzygają czy same identyfikatory internetowe, takie jak adresy IP czy identyfikatory plików cookies powinny być zawsze traktowane jako dane osobowe, czy jako jeden z czynników („śladów"), które mogą pozwolić na identyfikację osoby fizycznej (w motywie 30 RODO użyte jest zdanie „może (...) skutkować zostawieniem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystane do tworzenia profili i do identyfikowania tych osób").

- Nie ma podstaw by uznać, że adres IP (niezależnie od tego, czy jest adresem stałym (statycznym), czy zmiennym (dynamicznym)) oraz niezależnie od tego, kto jest jego dysponentem i jakie istnieją możliwości wykorzystania go w celu identyfikacji osoby fizycznej, należy zawsze traktować jako daną osobową. Ten sam wniosek dotyczy identyfikatorów plików cookies (aby móc to sprawdzić należy uwzględnić motyw 26 RODO).

Orzeczenie zdecydowanie zasługuje na uwagę – brakuje bowiem w Polsce rozstrzygnięć w tym przedmiocie. Wyrok budzi jednak uzasadnione wątpliwości, w szczególności w zakresie stanowiska sądu co do adresów IP. Wyrok nie jest prawomocny.

Ciekawe decyzje PUODO w trzecim kwartale 2022

W trzecim kwartale 2022 roku Prezes Urzędu Ochrony Danych Osobowych („PUODO") wydał szereg decyzji. Ich wspólnym mianownikiem były kryteria oceny ryzyka naruszenia praw osoby fizycznej przez administratora. Poniżej omówienie kilku szczególnie interesujących decyzji:

1. Decyzja w sprawie Esselmann Technika Pojazdowa sp. zo.o. sp. k.

W tym przypadku, administrator (Esselmann Technika Pojazdowa sp. zo.o. sp.k .) zagubił świadectwo pracy pracownika. Informacja o nieprawidłowościach związanych z przetwarzaniem danych osobowych u administratora została przekazana PUODO przez Komendanta Powiatowego Policji, a PUODO nałożył na administratora karę w wysokości 16 tys. zł w związku z niezgłoszeniem do organu naruszenia ochrony danych osobowych.

W uzasadnieniu wskazano, że zagubienie dokumentu tak istotnego jak świadectwo pracy i zawierającego tak dużą ilość informacji wiąże się z wysokim ryzykiem naruszenia praw i wolności osoby.

PUODO wskazał również, że przy ocenie ryzyka naruszenia, a w konsekwencji ocenie, czy administrator miał obowiązek zgłoszenia naruszenia do PUODO, nie jest istotny fakt, iż osoba, której dane dotyczyły nie zgłaszała do administratora roszczeń, a także, czy w toku postępowania ktoś faktycznie zapoznał się z danymi, ale czy wobec dokonanego naruszenia osoba trzecia miała teoretyczną możliwość się z utraconymi danymi zapoznać.

2. Trzecia kara dla Głównego Geodety Kraju

PUODO w dniu 6 lipca 2022 r. nałożył kolejną karę administracyjną o wysokości 60 tys. zł na Głównego Geodetę Kraju („GGK"). Podstawą kary było niezgłoszenie naruszenia do PUODO oraz zaniechanie poinformowania osób, których dane zostały ujawnione.

W pierwszych dniach kwietnia b.r. użytkownicy Internetu mogli przez ponad 48 godzin zapoznać się z numerami ksiąg wieczystych dostępnymi na stronie: www.geoportal.gov.pl

PUODO w komentowanej decyzji wskazał, że numery ksiąg wieczystych stanowią dane osobowe, gdyż te pozwalają bez nadmiernego wysiłku ustalić dane osobowe właścicieli nieruchomości, w tym: numery PESEL, imiona, nazwiska, imiona rodziców, a także adresy nieruchomości.

Decyzja potwierdza utrwaloną praktykę PUODO w zakresie traktowania numerów ksiąg wieczystych jako danych osobowych. W uzasadnieniu decyzji PUODO przywołuje orzeczenie Wojewódzkiego Sądu Administracyjnego w Warszawie (sygn. akt. II Sa/Wa 2222/20 [1]), zapadłe również w sprawie przeciwko GGK, w którym sąd ten potwierdził stanowisko organu, że numery ksiąg wieczystych są danymi osobowymi.

W uzasadnieniu decyzji PUODO wskazał również, że oceny ryzyka naruszenia praw lub wolności należy dokonać z punktu widzenia osoby dotkniętej naruszeniem, a nie z perspektywy interesów administratora, na co wskazywała zebrana w sprawie argumentacja GGK. Brak poinformowania osoby zainteresowanej o fakcie naruszenia uniemożliwia osobie dotkniętej naruszeniem możliwość prawidłowej oceny poziomu naruszenia jej praw. Tym samym niniejsze zaniechanie administratora należy oceniać wyjątkowo krytycznie.

3. Centrum Kliniczne Warszawskiego Uniwersytetu Medycznego

Powodem nałożenia przez organ 6 lipca 2022 r. kary w wysokości 10 tys. zł był brak zgłoszenia do PUODO naruszenia ochrony danych osobowych oraz niezawiadomienie o naruszeniu osoby, której dane dotyczą.

Naruszenie polegało na tym, że lekarz, będący pracownikiem administratora omyłkowo wpisał na skierowaniu do poradni specjalistycznej dane innego pacjenta. W toku postępowania, z uwagi na zidentyfikowaną pomyłkę w imieniu pacjenta, administrator uznał, że naruszenie nie miało miejsca, gdyż uniemożliwiała ona identyfikację osoby fizycznej, a zatem „naruszenie" dotyczyło osoby nieistniejącej. Na tej podstawie administrator zaniechał zgłoszenia naruszenia do PUODO oraz nie poinformował o naruszeniu osoby, której dane zostały omyłkowo ujawnione innemu pacjentowi.

Wobec faktu, że pozostałe dane ujawnione na skierowaniu pozwalały na identyfikację konkretnej osoby (nazwisko, adres zamieszkania i PESEL pacjenta), PUODO nie zgodził się z argumentacją administratora uznając, że doszło do naruszenia ochrony danych, które podlegało zgłoszeniu. Za wysokim ryzykiem naruszenia praw lub wolności osób przemawiał również w ocenie PUODO fakt, że dane będące przedmiotem wycieku były danymi szczególnymi w rozumieniu art. 9 RODO oraz należały do danych objętych tajemnicą lekarską.

W ocenie organu do nałożenia kary przyczynił się również fakt, iż administrator świadomie zaniechał realizacji obowiązków zgłoszeniowych.

Agata Szeliga
Partner, radca prawny
agata.szeliga@skslegal.pl
+48 698 660 648

Jakub Derulski
Prawnik, adwokat
jakub.derulski@skslegal.pl
+48 880 780 275

www.skslegal.pl