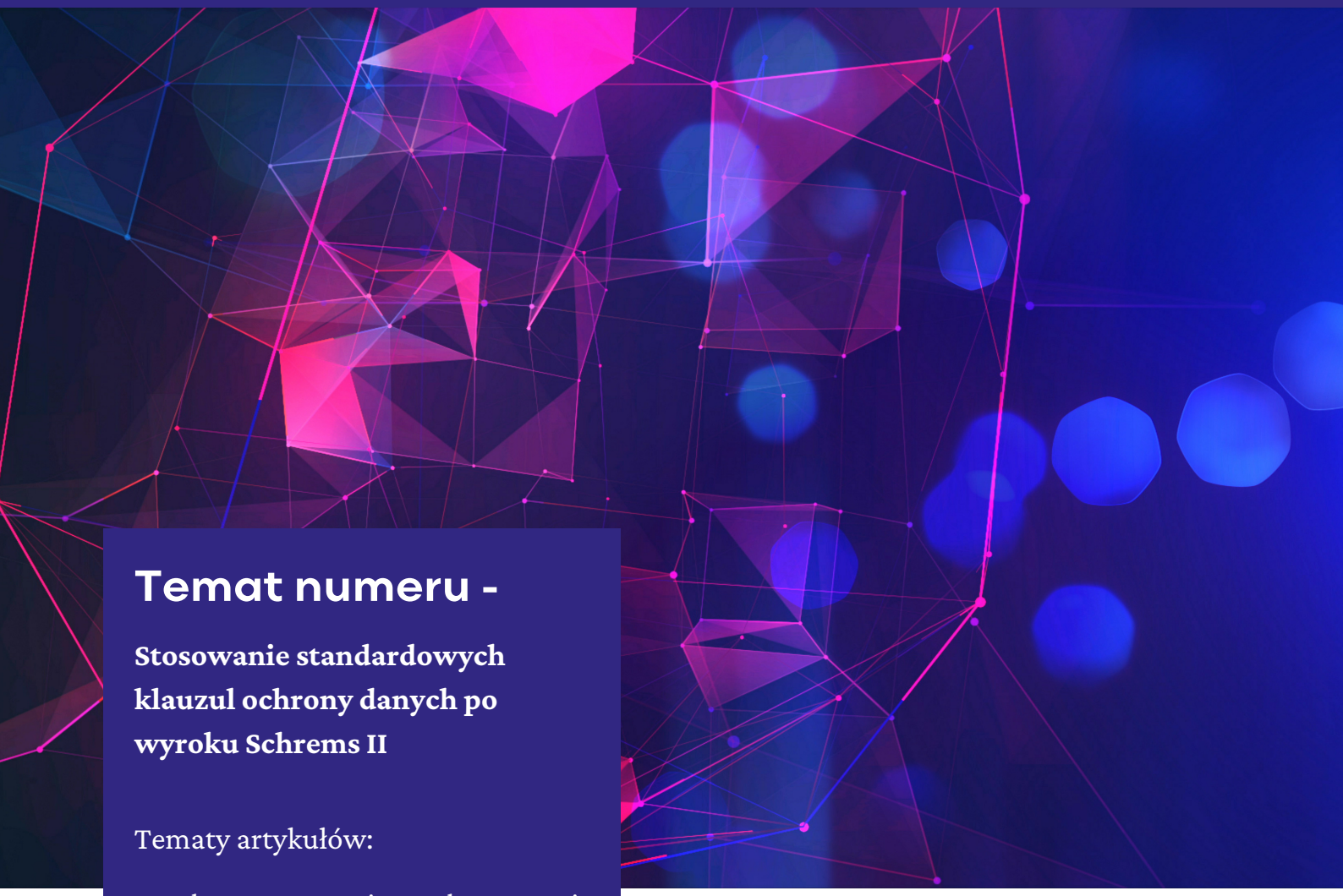
NR 3 - WRZESIEŃ 2020

NEWSLETTER RODO



Temat numeru -

Stosowanie standardowych klauzul ochrony danych po wyroku Schrems II

Tematy artykułów:

- Praktyczne znaczenie wyroku w sprawie Schrems II
- Duńskie standardowe klauzule powierzenia
- Brexit a wiążące reguły korporacyjne
- Naruszenia dotyczące braku współpracy z organem nadzorczym
- Stanowiska organów nadzorczych dot. biometrii
- Weryfikacja tożsamości osób a SI

Traple Konarski Podrecki & Wspólnicy

TKP

Znaczenie wyroku w sprawie Schrems II dla stosowania standardowych klauzul ochrony danych

adw. Xawery Konarski

Wyrok Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE, Trybunał) z dnia 16 lipca 2020 r. w sprawie Schrems II (dalej: wyrok Schrems II) zawiera kluczowe wskazówki dla eksporterów danych odnośnie do tego, jakich czynności powinni dokonać w przypadku oparcia transferu danych do państwa trzeciego na standardowych klauzulach ochrony danych, o których mowa w art. 46 ust. 2 pkt c) RODO. Odpowiadają one standardowym klauzulom umownym, przewidzianym w art. 25 ust. 4 dyrektywy 95/46/WE i zatwierdzonym decyzją Komisji Europejskiej – klauzule te pozostały w mocy po wejściu w życie RODO (art. 45 ust. 9 RODO), zmianie uległ jedynie sposób ich nazywania przez prawodawcę europejskiego.

W obecnym stanie prawnym to właśnie standardowe klauzule ochrony danych są najczęstszym mechanizmem transferowym, którym posługują się eksporterzy danych. Wynika to z kilku okoliczności. Po pierwsze, z faktu, że TSUE unieważnił decyzję Komisji Europejskiej nr 2016/1250 o odpowiedniości ochrony danych osobowych w przypadku transferu do Stanów Zjednoczonych wykonywanego na podstawie Tarczy Prywatności. Po drugie, do tej pory Komisja Europejska wydała decyzje stwierdzające odpowiedniość ochrony jedynie dla 12 państw (art. 45 ust. 1 RODO)[1] . Po trzecie, inne – niż standardowe klauzule ochrony danych – odpowiednie zabezpieczenia wymienione w art. 46 ust. 2 RODO albo mają ograniczony zakres zastosowania (wiążące reguły korporacyjne), albo też z braku odpowiednich decyzji Komisji Europejskiej lub organów nadzorczych nie są jeszcze dostępne dla eksporterów danych (np. jako zatwierdzone kodeksy postępowania).

Transfer danych na podstawie standardowych klauzul ochrony – uwagi ogólne

Wyrok TSUE w sprawie Schrems II dotyczy decyzji Komisji Europejskiej nr 2010/87/UE, regulującej transfer danych, w ramach którego eksporter danych jest administratorem, a importer danych z państwa trzeciego – podmiotem przetwarzającym. Nie ulega jednak wątpliwości, że zawarte w tym wyroku wskazówki znajdują zastosowanie również w przypadku pozostałych dwóch zestawów zatwierdzonych przez Komisję Europejską, a więc klauzul administrator–administrator, których dotyczą decyzje nr 2001/497/WE oraz nr 2004/915/WE[2].

Dla określenia dopuszczalności posługiwania się standardowymi klauzulami ochrony danych największe znaczenie mają wskazówki zawarte w motywie 126 uzasadnienia wyroku w sprawie Schrems II: „Choć zatem istnieją sytuacje, w których, w zależności od stanu prawnego i praktyk stosowanych w danym państwie trzecim, podmiot odbierający przekazywane w ten sposób dane jest w stanie zagwarantować ochronę danych, która jest konieczna, na podstawie samych standardowych klauzul ochrony danych, to jednak zachodzą inne sytuacje, w których postanowienia zawarte w tych klauzulach mogą nie stanowić wystarczającego środka pozwalającego na zapewnienie w praktyce skutecznej ochrony danych osobowych przekazywanych do danego państwa trzeciego. Ma to miejsce w szczególności wówczas, gdy prawo tego państwa trzeciego pozwala organom jego władzy publicznej na ingerencję w prawa osób, których te dane dotyczą”.

[1] W chwili obecnej takie decyzje zostały wydane dla Andory, Argentyny, Guernsey, Izraela, Jersey, Japonii, Kanady, Nowej Zelandii, Szwajcarii, Urugwaju, Wyspy Man, Wysp Owczych. W przygotowaniu jest decyzja dotycząca Korei Południowej.

[2] Przyjmuje się przy tym, że w przypadku transferów administrator-administrator, z racji autonomii importera danych w zakresie decyzji o ich dalszym przetwarzaniu, istnieje nawet większe ryzyko naruszenia interesów podmiotów danych. Może to mieć znaczenie przy ocenie, czy konieczne jest podjęcie „dodatkowych zabezpieczeń”, o których mowa w wyroku Schrems II – por. uwagi w dalszej części artykułu.

Po drugie, podmioty zaangażowane w transfer, a w szczególności eksporter danych, mają obowiązek dokonania uprzedniej analizy ustawodawstwa wewnętrznego importera danych, m.in. pod kątem zasad dostępu do przekazywanych danych podmiotów publicznych w tym państwie trzecim. Wymóg ten jest logiczną konsekwencją faktu, że – inaczej niż przy decyzji o adekwatności ochrony wydawanej na podstawie art. 45 ust. 1 RODO – Komisja Europejska, zatwierdzając standardowe klauzule ochrony, nie jest zobowiązana do przeprowadzenia oceny, czy państwa trzecie, do których dane osobowe mogłyby zostać przekazane na podstawie takich klauzul, zapewniają odpowiedni stopień ochrony. Celem zatwierdzenia klauzul przez Komisję jest bowiem jedynie zapewnienie ich spójności poprzez „jednolite ich zastosowanie we wszystkich państwach członkowskich, niezależnie od stopnia ochrony gwarantowanego w każdym z tych państw" (motyw 133 wyroku).

Po trzecie, gdy analiza ochrony danych w państwie trzecim da wynik negatywny, wówczas eksporter jest zobowiązany do zadbania o dodatkowe środki mające na celu zapewnienie przestrzegania odpowiedniego stopnia ochrony danych w państwie trzecim (motyw 133 wyroku). Jeśli nie może tego uczynić, to jest on – lub, pomocniczo, właściwy organ nadzorczy – zobowiązany do zawieszenia lub zakończenia przekazywania danych osobowych do danego państwa trzeciego.

Ustawodawstwo wewnętrzne i organ do spraw ochrony danych jako kryteria odpowiedniości ochrony danych osobowych w państwie trzecim

Zgodnie ze wskazówkami zawartymi w wyroku Schrems II elementy, które należy wziąć pod uwagę, dokonując oceny odpowiedniości ochrony w przypadku stosowania standardowych klauzul jako adekwatnego zabezpieczenia w rozumieniu art. 46 ust. 2 RODO, odpowiadają tym, które określone zostały w art. 45 ust. 2 RODO.

Zgodnie z art. 45 ust. 2 RODO, oceniając odpowiedniość ochrony w państwie trzecim, należy wziąć pod uwagę trzy elementy:

- ustawodawstwo wewnętrzne (ogólne lub sektorowe) w państwie trzecim, do którego przekazywane są dane,
- istnienie niezależnego organu do spraw ochrony danych osobowych oraz
- międzynarodowe zobowiązania danego państwa trzeciego.

Istotnych wskazówek w zakresie właściwego rozumienia pierwszych z powyższych elementów dostarcza nam ta część wyroku Schrems II, w której dokonano oceny ustawodawstwa

Stanów Zjednoczonych jako niespełniającego kryteriów należytej ochrony danych określonych prawem Unii Europejskiej. Nie kwestionując samej możliwości ograniczenia przez państwo trzecie prawa do prywatności i ochrony danych osobowych, np. z uwagi na interes bezpieczeństwa narodowego, Trybunał podkreślił jednocześnie, że ograniczenia takie muszą być zawężone do przypadków bezwzględnie koniecznych. Przepisy tego rodzaju powinny w szczególności określać jasne i precyzyjne zasady regulujące zakres stosowania ustanowionych ograniczeń praw podmiotów danych osobowych, a także wskazywać, w jakich okolicznościach i na jakich warunkach wyjątki te mają zastosowanie.

W powyższym kontekście eksporter danych powinien również ustalić, czy importer danych jest związany tego rodzaju przepisami, a także ocenić prawdopodobieństwo, że będzie on adresatem żądań opartych na tych przepisach ze strony podmiotów publicznych z terytorium, na którym ma on siedzibę. Pomocne w tym zakresie może być m.in. ustalenie takich okoliczności jak rodzaj transferowanych danych, cele ich przetwarzania przez importera, czas przechowywania danych w państwie trzecim, a także dotychczasowa praktyka ujawniania tego rodzaju informacji w państwie trzecim.

Z kolei jeżeli chodzi o wymóg funkcjonowania niezależnego organu do spraw ochrony danych w danym państwie trzecim, to nie należy go rozumieć jako konieczności ustanowienia odpowiednika organów nadzorczych w państwach Unii Europejskiej. Ważne jest jedynie to, aby organy te miały odpowiednią autonomię (tzn. nie podlegały władzy wykonawczej), a także by wydawane przez nie decyzje mogły być przez zainteresowane osoby zaskarżone do sądu.

Znaczenie ratyfikacji porozumień międzynarodowych przez państwo importera danych

Konieczność dokonania wyżej opisanej analizy stanu prawnego w państwie trzecim stanowi niewątpliwie istotną trudność dla eksporterów danych. Pomocna w związku z tym może być wskazówka wymieniona w art. 45 ust. 2 lit. c) RODO, zgodnie z którą przy dokonywaniu takiej oceny istotne znaczenie powinny mieć międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie. Przykładem zobowiązania tego

rodzaju, wymienionym wprost w motywie nr 105 RODO, jest Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych podpisana w Strasburgu dn. 28 stycznia 1981 r. Warto w związku z tym podkreślić, że Konwencję podpisało aż 55 państw, w tym 6 państw nieeuropejskich. Co więcej, w Komitecie Konwencji 108 w charakterze obserwatorów uczestniczy ponad 70 krajów. Choć ratyfikacja Konwencji stanowi istotny argument za stwierdzeniem odpowiedniości ochrony danych w państwie trzecim, to jednak automatyczne postępowanie w tym zakresie byłoby zbyt pochopne.

W powyższym kontekście odnotować należy jeszcze stanowisko brytyjskiego organu do spraw ochrony danych, który uznał, że przy ocenie odpowiedniości ochrony znaczenie ma okoliczność przyjęcia i wdrożenia przez dane państwo trzecie „Wytycznych dotyczących ochrony prywatności i przepływów transgranicznych danych osobowych", wydanych przez Organizację Współpracy Gospodarczej i Rozwoju (OECD).

Obowiązek wprowadzenia dodatkowych zabezpieczeń do standardowych klauzul ochrony

Zgodnie z motywem 126 uzasadnienia wyroku Schrems II w przypadku stwierdzenia braku odpowiedniości ochrony należy wprowadzić dodatkowe zabezpieczenia, oprócz tych zagwarantowanych standardowymi klauzulami ochrony. Taki sposób postępowania został generalnie zaaprobowany przez krajowe organy nadzorcze, w tym PUODO. Dotyczy to również transferów do Stanów Zjednoczonych, w których przypadku w wyroku Schrems II stwierdzono brak adekwatności ochrony w ustawodawstwie wewnętrznym. Odnotować jednak należy, że nieliczne organy odrzuciły taką konieczność (berliński rzecznik ochrony danych osobowych i holenderski rzecznik ochrony danych osobowych).

W dokumencie z dnia 24 lipca 2020 r. pt. „Najczęstsze pytania dotyczące wyroku Trybunału Sprawiedliwości Unii Europejskiej C-311/18 (Schrems II)" Europejska Rada Ochrony Danych (EROD) wskazała na trzy podstawowe rodzaje:

- organizacyjne,
- techniczne oraz
- prawne.

Przykładem rozwiązania organizacyjnego jest wdrożenie odpowiednich procedur związanych z zarządzaniem kluczami szyfrowania. Istotne znaczenie mogą mieć również posiadane przez importerów danych certyfikaty bezpieczeństwa (np. ISO/IEC 27001).

Typowym przykładem środka technicznego jest z kolei szyfrowanie danych, dokonywane zarówno podczas ich przechowywania (data at rest), używania (data in use), jak i w trakcie ich przesyłania (data in transit).

Do przykładowych środków prawnych zaliczyć należy z kolei te, które uzupełniają obowiązki wynikające z zatwierdzonych przez Komisję Europejską standardowych klauzul ochrony. Są to m.in.:

- obowiązek powiadamiania eksportera o żądaniach organów ścigania, wraz z przedstawieniem statystyk dotyczących częstotliwości i rodzaju wniosków realizowanych przez importera w okresie ostatniego roku / ostatnich dwóch lat, tak aby eksporter mógł ocenić prawdopodobieństwo, że również do jego danych służby uzyskają dostęp, oraz
- obowiązek poddania się kontroli/audytowi, tak aby eksporter danych mógł się upewnić, że importer ma odpowiednie procedury weryfikacji żądań podmiotów publicznych dotyczących wydania przekazanych przez eksportera danych osobowych.

Publikując powyższy dokument, EROD zadeklarowała jednocześnie rozpoczęcie prac nad wytycznymi dotyczącymi dodatkowych zabezpieczeń. Podobne oświadczenia złożyła również część organów nadzorczych państw Unii Europejskiej (np. Danii, Francji, Holandii, Irlandii).

Podsumowanie

W świetle treści wyroku w sprawie Schrems II obowiązki eksportera danych planującego oparcie transferu na standardowych klauzulach ochrony przedstawiają się następująco:

- Po pierwsze, eksporter danych powinien dokonać analizy odpowiedniości ochrony danych w państwie trzecim. Ocena ta powinna wziąć pod uwagę ustawodawstwo wewnętrzne w tym państwie, jak również okoliczności samego transferu danych (np. rodzaj przekazywanych informacji).
- Po drugie, w przypadku wątpliwości odnośnie do adekwatności ochrony w państwie trzecim eksporter powinien rozważyć wdrożenie dodatkowych, organizacyjnych, technicznych i prawnych, środków zabezpieczenia przekazywanych danych.
- Po trzecie, zgodnie z wymogami art. 5 ust. 2 RODO eksporter powinien należycie udokumentować wykonanie powyższych czynności, w tym wyniki dokonanej analizy. Przykładem działania wspierającego ten proces może być opracowanie kwestionariusza dla importerów danych, podobnego do materiałów tego rodzaju wykorzystywanych – zgodnie z art. 28 ust. 1 RODO – w procesie weryfikacji podmiotu przetwarzającego dane osobowe.

ORZECZNICTWO SĄDÓW KRAJOWYCH ORAZ WYTYCZNE I STANOWISKA ORGANÓW NADZORCZYCH

EROD wyjaśnia znaczenie wyroku w sprawie Schrems II

dr Iga Małobęcka-Szwast

Dnia 23 lipca 2020 r. podczas 36. posiedzenia plenarnego Europejska Rada Ochrony Danych (EROD) przyjęła dokument z najczęściej zadawanymi pytaniami (FAQ) dotyczącymi wyroku Trybunału Sprawiedliwości Unii Europejskiej (TSUE) w sprawie Schrems II. W artykule omawiamy najważniejsze wnioski wynikające z tego dokumentu dla stosowania instrumentów prawnych w celu przekazywania danych osobowych do państw trzecich (w tym do USA).

Główne tezy wyroku

EROD wskazuje na dwie główne tezy wyroku w sprawie Schrems II:

- Po pierwsze, TSUE stwierdził nieważność decyzji Komisji Europejskiej nr 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA. EROD podkreśla, że od chwili wydania wyroku przekazywanie danych osobowych do USA na podstawie ww. ram prawnych jest nielegalne.
- Po drugie, TSUE potwierdził ważność decyzji Komisji Europejskiej nr 2010/87 w sprawie standardowych klauzul umownych. Nałożono jednak na podmiot przekazujący dane i ich odbiorcę obowiązek sprawdzenia przed dokonaniem jakiegokolwiek przekazania danych, uwzględniając przy tym okoliczności przekazania, czy w danym państwie trzecim jest przestrzegany wymagany stopień ochrony w rozumieniu RODO. Jednocześnie TSUE stwierdził, że decyzja 2010/87/WE zobowiązuje importera danych do informowania podmiotu przekazującego dane (eksportera danych) o niemożności zastosowania się do standardowych klauzul ochrony danych i – w stosownych przypadkach – środków dodatkowych względem tych klauzul, w którym to przypadku to do podmiotu przekazującego dane należy zawieszenie przekazywania danych lub rozwiązanie umowy z importerem.

Dokładne omówienie wyroku TSUE znajduje się w artykule X. Konarskiego w lipcowym wydaniu newslettera RODO (Transfer danych osobowych do państwa trzeciego – znaczenie wyroku w sprawie Schrems II).

Stosowanie standardowych klauzul ochrony

Dalsze stosowanie standardowych klauzul ochrony w celu przekazywania danych do państwa trzeciego jest możliwe, należy jednak pamiętać, że próg określony przez TSUE w odniesieniu do przekazywania danych do USA ma zastosowanie do dowolnego państwa trzeciego.

TSUE podkreślił, że obowiązkiem podmiotu przekazującego dane i podmiotu je odbierającego jest dokonanie uprzedniej oceny, czy poziom ochrony wymagany prawem UE jest przestrzegany w danym państwie trzecim, co pozwoli ustalić, czy gwarancje przewidziane w standardowych klauzulach umownych mogą być przestrzegane w praktyce.

Jeżeli tak nie jest, należy przeanalizować, czy możliwe jest zastosowanie dodatkowych środków (dodatkowych zabezpieczeń) w celu zapewnienia „merytorycznie równoważnego" poziomu ochrony do poziomu przewidzianego w RODO, jak również, czy prawo państwa trzeciego nie wpłynie niekorzystnie na takie dodatkowe środki, pozbawiając je skuteczności.

EROD rekomenduje, aby w celu dokonania weryfikacji przepisów w państwie trzecim podmiot przekazujący dane skontaktował się z podmiotem odbierającym dane i podjął z nim współpracę na potrzeby takiej oceny.

Dodatkowe zabezpieczenia

TSUE podkreślił, że jeżeli w następstwie dokonania oceny prawa państwa trzeciego podmiot przekazujący dane i podmiot odbierający dane dojdą do wniosku, że standardowe klauzule umowne lub wiążące reguły korporacyjne nie zapewniają same w sobie dostatecznego poziomu gwarancji, podmioty te zobowiązane są do zapewnienia niezbędnych dodatkowych środków (dodatkowych zabezpieczeń), które pozwolą na zagwarantowanie odpowiedniego poziomu ochrony osób fizycznych w rozumieniu RODO.

Takie środki powinny być przedstawiane indywidualnie dla każdego przypadku z uwzględnieniem wszystkich okoliczności przekazywania danych oraz po dokonaniu oceny prawa państwa trzeciego służącej zweryfikowaniu, czy zapewnia ono odpowiedni poziom ochrony. EROD wskazuje, że dodatkowe zabezpieczenia mogą mieć charakter środków prawnych, technicznych lub organizacyjnych, które można zapewnić jako uzupełnienie standardowych klauzul umownych lub wiążących reguł korporacyjnych w celu przekazywania danych do państw trzecich, w sytuacji gdy uprzednia ocena standardowych klauzul umownych lub wiążących reguł korporacyjnych dokonana przez eksportera i importera danych doprowadzi do wniosku, że mechanizmy te nie zapewniają dostatecznego poziomu ochrony.

Co istotne, jeżeli eksporter i importer danych – uwzględniając okoliczności przekazywania danych i ewentualne środki dodatkowe – stwierdzą, że nie jest możliwe zapewnienie odpowiednich zabezpieczeń, mają oni obowiązek zawiesić lub zakończyć przekazywanie danych osobowych.

Z racji tego, że nie jest jasne, na czym owe „dodatkowe środki" miałyby polegać, EROD zapowiedziała wydanie w tym zakresie odpowiednich wytycznych.

Wpływ wyroku TSUE na pozostałe narzędzia transferu danych

EROD podkreśla, że kryteria ustalone przez TSUE w wyroku w sprawie Schrems II w odniesieniu do państw trzecich mają zastosowanie do wszystkich odpowiednich zabezpieczeń z art. 46 RODO[1] wykorzystywanych do przekazywania danych z EOG do dowolnego państwa trzeciego.

W szczególności ocena TSUE ma zastosowanie również do wiążących reguł korporacyjnych. To, czy przekazywanie danych osobowych na podstawie wiążących reguł korporacyjnych będzie możliwe, zależeć będzie od wyniku oceny dokonanej z uwzględnieniem okoliczności przekazywania danych i dodatkowych środków, które można zastosować, aby zapewnić odpowiedni poziom ochrony osób fizycznych.

Te dodatkowe środki, w połączeniu z wiążącymi regułami korporacyjnymi, przyjęte w następstwie indywidualnej analizy okoliczności towarzyszących przekazywaniu danych, muszą zagwarantować, by prawo państwa trzeciego nie wpływało niekorzystnie na odpowiedni poziom zapewnionej przez te środki ochrony.

EROD dokona oceny skutków wyroku dla narzędzi przekazywania danych innych niż standardowe klauzule umowne i wiążące reguły korporacyjne. W wyroku doprecyzowano, że standardem w przypadku odpowiednich zabezpieczeń z art. 46 RODO jest „merytoryczna równoważność" stopnia ochrony z tym, jaki jest gwarantowany w Unii przez RODO. W ocenie TSUE z racji tego, że art. 46 znajduje się w rozdziale V RODO, należy go odczytywać w świetle art. 44 RODO, który stanowi, że „wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu".

EROD zapowiedziała, że będzie uzupełniać dokument FAQ o kolejne wskazówki wraz z dalszą analizą treści wyroku TSUE w sprawie Schrems II.

Źródło:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_faqs_schrems_ii_202007_adopted_pl.pdf.

[1] 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).

Jak stosować duńskie standardowe klauzule powierzenia przetwarzania – ocena przyjętych rozwiązań

adw. dr hab. Grzegorz Sibiga i adw. Katarzyna Syska

Duńskie standardowe klauzule umowne dotyczące powierzenia przetwarzania danych są jak dotąd jedynymi klauzulami, które mają status standardowych klauzul ochrony danych w rozumieniu art. 28 ust. 8 RODO[1].

Ich obecna wersja została przyjęta po wprowadzeniu zmian wynikających z opinii Europejskiej Rady Ochrony Danych (EROD) w sprawie projektu klauzul.

Zarówno w klauzulach, jak i w opinii EROD znajdują się liczne wskazówki co do tego, jak z tych standardowych klauzul należy korzystać. Poniżej przedstawiamy ich strukturę i wskazujemy, jak można je dostosować do własnych potrzeb.

Status klauzul

Standardowe klauzule umowne stanowią mechanizm zapewniania zgodności z warunkami powierzenia przetwarzania danych osobowych określonymi w art. 28 ust. 3–4 RODO. W RODO przewiduje się dwa rodzaje takich klauzul, według kryterium organu je przyjmującego. Organem tworzącym i przyjmującym standardowe klauzule może być Komisja Europejska (art. 28 ust. 7 RODO) lub organ nadzorczy w państwie członkowskim (art. 28 ust. 8 RODO). W tym drugim przypadku w procedurze przyjmowania klauzul uczestniczy EROD, która wydaje opinię w ich sprawie (art. 64 ust. 1 lit. d RODO).

Korzystanie ze standardowych klauzul jest jedynie opcją dla stron umowy, ponieważ alternatywnie mogą one tworzyć umowy indywidualne. Zastosowanie standardowych klauzul gwarantuje jednak zgodność z warunkami z art. 28 ust. 3–4 RODO, o ile załączniki do klauzul są prawidłowo uzupełnione. W ramach Unii Europejskiej (tj. w jej państwach członkowskich) korzystanie z klauzul, ich moc konsekwencje stosowania nie są w żaden sposób ograniczone terytorialnie. Nie ma zatem znaczenia, że klauzule te przyjął duński organ nadzorczy – mogą je stosować podmioty z całej UE i powoływać się na zgodność klauzul z RODO.

Zgodnie ze stanowiskiem EROD strony mogą także dodawać inne klauzule lub dodatkowe gwarancje, pod warunkiem że nie są one sprzeczne,bezpośrednio lub pośrednio, z przyjętymi standardowymi klauzulami umownymi ani nie naruszają podstawowych praw i wolności osób, których dane dotyczą. Pod tymi warunkami zastosowanie dodatkowych postanowień nie wpływa negatywnie na skuteczność stosowania standardowych klauzul jako mechanizmu zgodności. Natomiast nie można się skutecznie powoływać na zastosowanie klauzul jako mechanizmu zgodności, jeżeli strony umowy dokonały zmian w ich treści.

Struktura klauzul

Duńskie standardowe klauzule umowne można podzielić na dwie części: ogólną i szczegółową.

Część ogólna zawiera postanowienia, które zasadniczo nie wymagają uzupełnień. Są to między innymi postanowienia dotyczące zobowiązania podmiotu przetwarzającego do działania zgodnie z poleceniami administratora, zobowiązania do zachowania poufności, korzystania z podwykonawców.

Natomiast część szczegółowa składa się z czterech załączników (A–D), które należy uzupełnić w taki sposób, aby odpowiadały one kontekstowi konkretnej sytuacji powierzenia przetwarzania danych. W załącznikach należy wskazać między innymi cel przetwarzania, rodzaj danych osobowych oraz kategorie podmiotów danych, polecenia administratora dotyczące na przykład stosowanych środków zabezpieczających, wsparcia administratora w realizacji żądań podmiotów danych i w realizacji wymogów z art. 32–36 RODO.

[1] 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).

Dostosowywanie klauzul do kontekstu i charakteru przetwarzania

Duńskie standardowe klauzule umowne wymagają uzupełnienia i dostosowania do konkretnego przypadku powierzenia przetwarzania. Dotyczy to w szczególności załącznika C zatytułowanego „Polecenia dotyczące wykorzystania danych osobowych".

W załączniku tym należy określić szczegółowe prawa i obowiązki stron dotyczące między innymi środków zabezpieczających, przeprowadzania audytów, wspierania administratora w realizacji żądań podmiotów danych i w realizacji wymogów z art. 32–36 RODO.

Załącznik C oraz opinia EROD zawierają przykładowe postanowienia w powyższym zakresie lub wskazówki co do tego, jak poszczególne kwestie powinny być uregulowane.

Na przykład w odniesieniu do obowiązku wspierania administratora w realizacji żądań podmiotów danych można uregulować między innymi następujące kwestie:

- w jaki sposób i w jakim terminie podmiot przetwarzający ma poinformować administratora o tym, że otrzymał wniosek podmiotu danych;
- czy podmiot przetwarzający ma odpowiadać na wnioski podmiotów danych w imieniu administratora, a jeśli tak, to według jakich zasad lub procedury;
- czy podmiot przetwarzający jest zobowiązany do wdrożenia rozwiązań technicznych pozwalających podmiotom danych na realizację swoich praw, na przykład prawa dostępu do danych.

W zależności od okoliczności powierzenia szczegółowe polecenia administratora i obowiązki podmiotu przetwarzającego powinny się odpowiednio różnić.

Duński organ nadzorczy nie zaproponował zatem uniwersalnego zestawu postanowień umownych, które można by zastosować w każdej sytuacji bez żadnych zmian czy uzupełnień. Wydaje się, że organ uznał za niemożliwe przygotowanie wzoru umowy na każdą okoliczność oraz że prawidłową realizacją wymogów RODO jest dopasowywanie praw i obowiązków stron do okoliczności powierzenia przetwarzania.

Ocena przydatności klauzul

Standardowe klauzule duńskiego organu nadzorczego są pierwszymi standardowymi klauzulami powierzenia w UE. Są one o tyle istotne, że wskazują sposób zapewnienia zgodności z art. 28 ust. 3–4 RODO. Zastosowanie klauzul przez strony nie jest jednak prostym działaniem polegającym na ich przeniesieniu do treści umowy, ponieważ wymagają one dopasowania do konkretnego przypadku powierzenia przetwarzania i jego specyfiki. W swojej znaczącej części załączniki (A–D), a w pewnych elementach część główna, wymagają uzupełnienia przez strony umowy. Dopiero poprawne ich uzupełnienie zagwarantuje zgodność z art. 28 ust. 3–4 RODO, a strony będą mogły skutecznie powoływać się na ten mechanizm zgodności.

Jak już wspomnieliśmy, przyjęty standard może być przez strony uzupełniany dodatkowymi klauzulami i gwarancjami, które nie są sprzeczne z tym standardem ani nie naruszają podstawowych praw i wolności podmiotu danych.

Natomiast nawet jeśli strony umowy nie zdecydują się na skorzystanie z całych standardowych klauzul, ale tylko z niektórych ich elementów, to w naszej ocenie i tak klauzule stanowią cenną wskazówkę, jak prawidłowo realizować poszczególne wymagania powierzenia przetwarzania danych osobowych. Oczywiście na gruncie formalnym należy wówczas pamiętać, że takie częściowe użycie klauzul nie daje możliwości skutecznego powoływania się na zastosowanie standardowych klauzul.

Brexit a wiążące reguły korporacyjne

r. pr. Dominika Nowak

Dnia 22 lipca 2020 r. podczas 35. posiedzenia plenarnego Europejska Rada Ochrony Danych (EROD) przyjęła notę informacyjną dotyczącą działań, które należy podjąć, aby zapewnić, że wiążące reguły korporacyjne mogą być nadal wykorzystywane jako ważne narzędzie przekazywania danych do państw trzecich po zakończeniu tzw. okresu przejściowego związanego z brexitem.

W związku z tym, że brytyjski organ nadzorczy nie będzie już kwalifikowany jako właściwy na mocy RODO, decyzje zatwierdzające podjęte przez brytyjski organ nadzorczy nie będą już miały mocy prawnej na terytorium Europejskiego Obszaru Gospodarczego (EOG).

Ponadto zmian może wymagać treść wiążących reguł korporacyjnych, ponieważ zawierają one odniesienia do brytyjskiego porządku prawnego. Dotyczy to również wiążących reguł korporacyjnych zatwierdzonych na mocy dyrektywy 95/46/WE.

Podmioty korzystające z wiążących reguł korporacyjnych, dla których brytyjski organ nadzorczy był do tej pory organem wiodącym, powinny ustalić nowy organ wiodący w tym zakresie. Zmiana organu wiodącego powinna nastąpić przed końcem okresu przejściowego, czyli do 31 grudnia 2020 r.

Podmioty, które obecnie wnioskują o zatwierdzenie wiążących reguł korporacyjnych, powinny również poczynić ustalenia w celu zidentyfikowania na terytorium EOG nowego organu wiodącego, z którym należy się skontaktować w celu przekazania informacji o tym, dlaczego dany organ nadzorczy powinien być traktowany jako wiodący.

Wiążące reguły korporacyjne zatwierdzone przez brytyjski organ nadzorczy zgodnie z RODO będą podlegać zatwierdzaniu przez nowy organ wiodący z państwa członkowskiego EOG przed końcem okresu przejściowego, po uzyskaniu opinii EROD.

EROD przyjęła również załącznik zawierający listę kontrolną elementów, które należy zmienić w dokumentach dotyczących wiążących reguł korporacyjnych w związku z brexitem.

Link do informacji: https://edpb.europa.eu/news/news/2020/european-data-protection-board-thirty-fifth-plenary-session-information-note-binding_en.

Link do noty informacyjnej: https://edpb.europa.eu/sites/

Stanowiska unijnych organów dotyczące biometrii, w tym technologii rozpoznawania twarzy (FRT)

Mateusz Kupiec

Stosowanie systemów biometrycznych, w tym technologii rozpoznawania twarzy, w celu identyfikacji lub weryfikacji tożsamości zyskuje w ostatnim czasie na popularności. Korzystanie z takich rozwiązań wiąże się jednak z przetwarzaniem szczególnej kategorii danych osobowych i znaczącą ingerencją w autonomię informacyjną osób fizycznych. Przedstawiamy ostatnie opinie i wytyczne unijnych organów zajmujących się ochroną danych osobowych.

Przed analizą poszczególnych stanowisk organów warto wyjaśnić, czym właściwie są systemy biometryczne oraz technologie rozpoznawania twarzy.

Czym są systemy biometryczne?

W dokumencie roboczym Grupy Roboczej Art. 29 dotyczącym biometrii (WP 80) systemy biometryczne zostały zdefiniowane jako „aplikacje wykorzystujące technologie biometryczne, które umożliwiają automatyczną identyfikację lub uwierzytelnienie/weryfikację danej osoby".

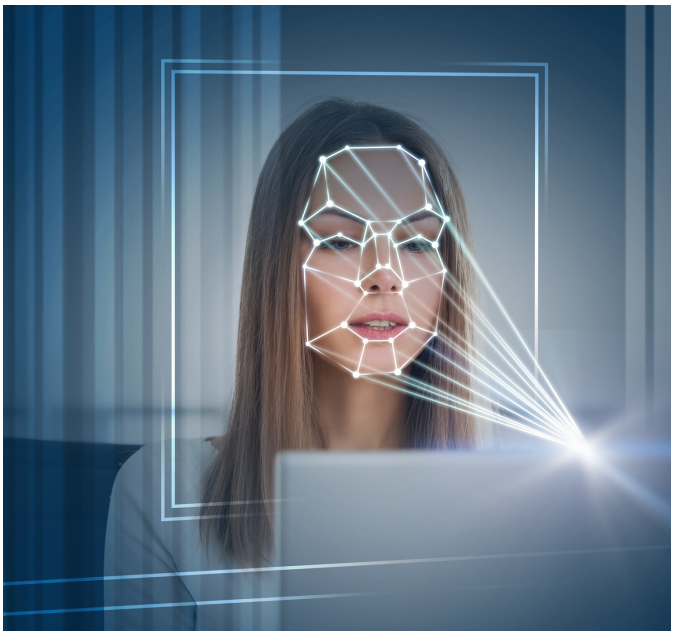
Funkcjonowanie tych systemów oparte jest więc na przetwarzaniu danych biometrycznych, czyli takich danych osobowych, które:

- wynikają ze specjalnego przetwarzania technicznego;
- dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej;
- umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, np. wizerunek twarzy lub dane daktyloskopijne (art. 4 pkt 14 RODO[1]).

Należy przypomnieć, że przetwarzanie danych biometrycznych jako szczególnej kategorii danych osobowych wymaga od administratora tych danych ustalenia zarówno podstawy z art. 6 ust. 1 RODO, jak i dodatkowej podstawy (warunku dopuszczalności) z art. 9 ust. 2 RODO.

Czym jest FRT?

Pod pojęciem technologii rozpoznawania twarzy rozumie się systemy biometryczne wykorzystujące sztuczną inteligencję w celu rozpoznania i następnie przetworzenia rysów twarzy danej osoby. Oznacza to, że technologie rozpoznawania twarzy również wykorzystują dane biometryczne. Systemy wykorzystujące FRT są najczęściej wdrażane przez prywatne przedsiębiorstwa oraz podmioty publiczne, aby np. bardziej skutecznie kontrolować dostęp do określonych pomieszczeń. Jednakże coraz częściej rozwiązania te stosuje się w celach związanych z zarządzaniem relacjami z klientem (CRM) lub personalizacją doświadczeń konsumenta.



Raport AEPD ws. stosowania FRT podczas egzaminów na studiach

Hiszpański organ nadzorczy (AEPD) opublikował w maju 2020 r. analizę dotyczącą stosowania przez uniwersytety technologii rozpoznawania twarzy w celu identyfikacji studentów przystępujących do egzaminów w warunkach online. Zdaniem organu:

- wyraźna zgoda studentów będzie stanowić ważną podstawę przetwarzania ich danych biometrycznych, gdy zgoda ta będzie dobrowolna, konkretna, świadoma i jednoznaczna;
- studenci będą mogli wyrazić zgodę dobrowolnie jedynie wtedy, gdy uczelnia przedstawi im porównywalny alternatywny sposób weryfikacji ich tożsamości, który nie będzie wymagał przetwarzania danych biometrycznych;

[1] 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).

- inne możliwości identyfikacji zaprezentowane studentom muszą odpowiadać rozwiązaniom wykorzystującym FRT pod względem czasu trwania procesu oraz skomplikowania (trudności użycia);
- podstawą prawną dla przetwarzania danych biometrycznych w ramach systemu FRT w wyżej wskazanych celach mogłaby być również niezbędność procesu ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, proporcjonalnych do wyznaczonego celu, nienaruszających istoty prawa do ochrony danych i przewidujących odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Wspólny dokument AEPD i EIOD w sprawie 14 nieporozumień dotyczących identyfikacji biometrycznej i uwierzytelniania

W czerwcu 2020 r. hiszpański organ nadzorczy (AEPD) oraz Europejski Inspektor Ochrony Danych (EIOD) opublikowali dokument, w którym zwracają uwagę m.in., że:

- identyfikacja za pomocą technologii biometrycznych nie zawsze jest dokładna;
- w odróżnieniu od tradycyjnych haseł dane biometryczne zebrane podczas uwierzytelniania lub procedury identyfikacji ujawniają więcej informacji na temat osoby, której dane dotyczą;
- identyfikacja lub weryfikacja tożsamości za pomocą technologii biometrycznej nie jest odpowiednia dla każdej osoby;
- niektóre osoby nie mogą korzystać z niektórych rodzajów danych biometrycznych, ponieważ cechy fizyczne tych osób nie są rozpoznawane przez system – przypadku niektórych urazów, chorób taka niezgodność może mieć charakter stały;
- istnieją metody, które pozwalają na ominięcie biometrycznych systemów uwierzytelniania i przyjęcie tożsamości innej osoby;
- systemy biometryczne mogą mieć problemy w odróżnieniu spokrewnionych ze sobą osób, np. rodzeństwa.

Komentarz

Systemy biometryczne, w tym technologie rozpoznawania twarzy, są stosowane coraz częściej jako metody identyfikacji lub weryfikacji tożsamości. Zwracamy uwagę, że decydując się na korzystanie z takich rozwiązań w swojej organizacji, administratorzy danych osobowych muszą ustalić właściwą podstawę przetwarzania danych osobowych oraz przeprowadzić i udokumentować odpowiednio wcześniej ocenę skutków dla ochrony danych (DPIA). Przetwarzanie danych osobowych przy użyciu tych technologii ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może bowiem powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 ust. 1 RODO).

Weryfikacja tożsamości osób, których dane dotyczą, na etapie trenowania modelu uczenia maszynowego – wytyczne ICO

Mateusz Kupiec

Funkcjonowanie sztucznej inteligencji (SI) wymaga przetwarzania danych, w tym nierzadko danych osobowych. Osoby, których dane dotyczą, stają się coraz bardziej świadome swoich praw wynikających z RODO, dlatego należy oczekiwać, że liczba wniosków o realizację tych praw, skierowanych do podmiotów wykorzystujących systemy sztucznej inteligencji, będzie systematycznie rosnąć – szczególnie na etapie trenowania modelu uczenia maszynowego. Brytyjski organ nadzorczy (ICO) w swoich wytycznych dotyczących SI i ochrony danych wskazuje na problem identyfikacji osób fizycznych, których dane są przetwarzane w ramach modeli uczenia maszynowego, i udziela wskazówek w tym zakresie.

Sztuczna inteligencja, uczenie maszynowe i dane osobowe

W obecnym porządku prawnym brakuje powszechnie obowiązującej definicji sztucznej inteligencji. W dokumencie Komisji Europejskiej pt. *Sztuczna inteligencja dla Europy* zaproponowano, że termin SI „odnosi się do systemów, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowaniu działań – do pewnego stopnia autonomicznie – w celu osiągnięcia konkretnych celów". Jednocześnie, jak trafnie zauważa ICO, w opublikowanych wytycznych dotyczących SI i ochrony danych (*Guidance on AI and data protection*) pojęcie to ma ogólny charakter (*umbrella term*) i zazwyczaj jest ono używane w kontekście systemów uczenia maszynowego (*machine learning*), które stanowią istotny obszar sztucznej inteligencji. Uczenie maszynowe organ definiuje jako „zestaw technik i narzędzi, które umożliwiają maszynom »myślenie« poprzez tworzenie algorytmów matematycznych opartych na zgromadzonych danych".

Uczenie maszynowe stanowi więc dziedzinę sztucznej inteligencji, która na podstawie wyszukiwania relacji w danych treningowych (*training data*) stara się naśladować inteligentne zachowania (np. rozpoznawanie mowy). W związku z tym wydaje się, że obecnie najważniejszym elementem sztucznej inteligencji i związanych z nią modeli uczenia maszynowego jest zdolność samodzielnego rozwiązywania problemów podczas procesu naśladującego ludzkie myślenie. Niezależnie od wytycznych ICO warto w tym miejscu zauważyć, że w celu „nauczenia" konkretnego systemu SI określonego zachowania w zależności od charakteru analizowanego przez niego problemu biznesowego opracowano cztery główne metody uczenia maszynowego, o których wyborze powinien decydować rodzaj i rozmiar danych przetwarzanych przez konkretny system:

- uczenie nadzorowane;
- uczenie częściowo nadzorowane;
- uczenie nienadzorowane;
- uczenie przez wzmacnianie.

ICO zakłada, że podmiot tworzący modele uczenia maszynowego lub korzystający z nich niezmiennie będzie potrzebował danych treningowych niezbędnych do „wytrenowania" algorytmu uczenia maszynowego. Gdy tymi informacjami będą dane osobowe, zastosowanie znajdą przepisy RODO (art. 2 ust. 1 RODO). Osoba, której dane dotyczą, będzie więc mogła w takim przypadku skutecznie skorzystać z praw, jakie gwarantuje jej RODO, chyba że administrator danych osobowych nie będzie w stanie jej zidentyfikować lub w konkretnej sytuacji przetwarzania danych określone prawo będzie podlegać ograniczeniu.

[1] 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).

Dane treningowe a identyfikacja osoby, której dane dotyczą

Trenowanie modelu uczenia maszynowego polega w uproszczeniu na „uczeniu się" przez niego zależności i szukaniu nowych rozwiązań dla wyznaczonych mu problemów na podstawie danych, którymi dysponuje. Proces ten rozpoczyna się od wprowadzenia danych szkoleniowych do wybranego algorytmu. Jak wskazuje ICO, dane treningowe zawierają zazwyczaj informacje niezbędne do dokonywania prognozy zachowania jednostek, np. dane o lokalizacji określonej osoby, a nie ich dane kontaktowe. Co więcej, wykorzystywane dane treningowe często poddawane są różnym pomiarom, przekształceniom, aby analiza tych danych była łatwiejsza dla algorytmów uczenia maszynowego – proces ten określa się mianem przetwarzania wstępnego (*pre-processing*).

W opublikowanych wytycznych ICO zauważa, że przekształcanie danych osobowych z jednej formy w inną (potencjalnie mniej szczegółową) może spowodować, że dane treningowe trudniej będzie powiązać z konkretną osobą fizyczną. Tym samym administrator danych osobowych może mieć trudności z identyfikacją osoby, która żąda od niego np. usunięcia danych. Jednakże zdaniem organu takie przetworzone dane wciąż będą danymi osobowymi w rozumieniu RODO, gdy będą mogły one zostać samodzielnie (lub w zestawieniu z innymi danymi przetwarzanymi przez konkretny podmiot) wykorzystane do „wyodrębnienia" (*single-out*) określonej osoby, której dane dotyczą, z pewnej grupy.

W celu plastycznego przedstawienia takiej sytuacji ICO posłużył się przykładem danych treningowych wykorzystanych w modelu służącym do prognozowania zakupów (*purchase prediction model*). W przypadku gdy zestaw takich danych zawiera unikatowy wzór zachowania zakupowego konkretnej osoby, a osoba występująca z wnioskiem o realizację prawa wynikającego z RODO załączy do niego historię swoich ostatnich zakupów, to administrator danych osobowych będzie mógł określić, czy przetwarza informacje dotyczące tej osoby.

Komentarz

Weryfikacja tożsamości osoby występującej z żądaniem realizacji prawa przysługującego jej na podstawie RODO jest częstym problemem, z jakim spotykają się administratorzy danych osobowych. Nie mogą oni bowiem merytorycznie odnieść się do żądania podmiotu danych, jeżeli nie są w stanie jednoznacznie stwierdzić, czy przetwarzają jego dane osobowe, lub gdy nie mogą ustalić tożsamości wnioskodawcy. Trenowanie modeli uczenia maszynowego stanowi czasochłonny proces, podczas którego administrator danych osobowych nierzadko będzie musiał się odnieść do żądań osób, których dane osobowe wykorzystuje w tym procesie. Z tego względu podmioty tworzące modele uczenia maszynowego lub korzystające z takich rozwiązań, w ramach których wykorzystują dane osobowe, powinny jak najszybciej opracować i wdrożyć zasady postępowania dotyczące wniosków osób, których dane dotyczą.

Naruszenia ochrony danych osobowych dotyczące braku współpracy z organem nadzorczym

r.pr. Dominika Nowak

Od marca do lipca 2020 r. Prezes Urzędu Ochrony Danych Osobowych (UODO) wydał cztery decyzje nakładające administracyjne kary pieniężne za brak współpracy z organem. Warto zapoznać się z okolicznościami nałożenia poszczególnych kar, aby w przypadku ewentualnej kontroli lub wezwania otrzymanego od organu nie narazić się na taki zarzut i związane z nim konsekwencje.

Na wstępie należy przypomnieć, że zgodnie z art. 31 RODO[1] „administrator i podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań".

Komplementarne dla tych obowiązków są uprawnienia organu nadzorczego polegające m.in. na uzyskiwaniu od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań oraz uzyskiwaniu dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego (art. 58 ust.1 lit. e i f RODO).

Opisy naruszeń ochrony danych osobowych

- **Vis Consulting sp. z o.o. w likwidacji (ZSPR.421.19.2019)**

9 marca 2020 r. Prezes UODO wydał decyzję w sprawie Vis Consulting sp. z o.o. w likwidacji z siedzibą w Katowicach, nakładającą administracyjną karę pieniężną w wysokości 20 000 zł.

W ocenie organu adresat decyzji naruszył art. 31 RODO oraz art. 58 ust. 1 lit. e i f RODO poprzez niezapewnienie inspektorom dostępu do danych osobowych i innych informacji oraz pomieszczeń, co skutkowało uniemożliwieniem przeprowadzania czynności kontrolnych niezbędnych do realizacji zadań tych inspektorów.

Nakładając administracyjną karę pieniężną, Prezes UODO wziął pod uwagę, że:

- po uzyskaniu informacji o planowanej kontroli Prezesa UODO spółka skierowała do wynajmującego wniosek o rozwiązanie umowy najmu na lokal;
- spółka dwukrotnie udaremniła przeprowadzenie czynności kontrolnych, gdyż kontrolerzy nie zastali przedstawicieli spółki pod adresem wskazanym w KRS;
- po uzyskaniu informacji o planowanej kontroli podjęto uchwałę o rozwiązaniu spółki i rozpoczęciu postępowania likwidacyjnego.

Te działania spółki uniemożliwiły Prezesowi UODO wykonywanie obowiązków nałożonych przez przepisy prawa.

- **East Power sp. z o.o. (DKE.561.1.2020)**

29 maja 2020 r. Prezes UODO wydał decyzję w sprawie East Power sp. z o.o. z siedzibą w Jeleniej Górze, nakładającą administracyjną karę pieniężną w wysokości 15 000 zł.

Adresat decyzji naruszył art. 31 RODO oraz art. 58 ust. 1 lit. e RODO poprzez niezapewnienie dostępu do danych osobowych i innych informacji niezbędnych do realizacji i innych

[1] 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).

informacji niezbędnych do realizacji zadań przez organ nadzorczy, w tym do rozpatrzenia skargi osoby, której dane dotyczą.

Nakładając administracyjną karę pieniężną, Prezes UODO wziął pod uwagę, że:
spółka dwukrotnie nie udzieliła wyjaśnień na wezwanie Prezesa UODO;
na jedno wezwanie udzielono odpowiedzi niepełnej, która nie uwzględniała zadanych szczegółowych pytań;
spółka udzieliła odpowiedzi, które nie wyjaśniły stanu faktycznego, lecz spowodowały dodatkowe wątpliwości.

Te działania spółki zostały uznane za utrudnienie i uniemożliwienie uzyskania przez organ nadzorczy informacji, co skutkuje również nadmiernym i nieuzasadnionym przedłużaniem postępowania, co stoi w sprzeczności z podstawowymi zasadami rządzącymi postępowaniem administracyjnym.

- **Pani A. T. prowadząca działalność gospodarczą pod nazwą [...] w Ł. (Niepubliczny Żłobek i Przedszkole) (DKE.561.2.2020)**

3 czerwca 2020 r. Prezes UODO wydał decyzję w sprawie osoby prowadzącej jednoosobową działalność gospodarczą (Niepubliczny Żłobek i Przedszkole), nakładającą administracyjną karę pieniężną w wysokości 5000 zł.

Adresat decyzji naruszył art. 31 RODO oraz art. 58 ust. 1 lit. e RODO poprzez niezapewnienie dostępu do danych osobowych i innych informacji niezbędnych organowi nadzorczemu do realizacji jego zadań, tj. oceny naruszenia ochrony danych osobowych na podstawie art. 34 ust. 1 i 2 RODO zgłoszonego przez adresata decyzji.

Nakładając administracyjną karę pieniężną, Prezes UODO wziął pod uwagę, że:
- administrator nie udzielił odpowiedzi na żadne z trzech wysłanych przez organ nadzorczy wezwań dotyczących przedstawienia zanonimizowanej treści zawiadomienia o naruszeniu ochrony danych osobowych;
- żadne z tych wezwań nie zostało odebrane, pomimo że adresat wcześniej zgłosił naruszenie ochrony danych i mógł się spodziewać kontaktu ze strony Prezesa UODO;
- adresat decyzji nie próbował usprawiedliwić braku odpowiedzi na wezwania.

- **Główny Geodeta Kraju z siedzibą w Warszawie (DKE.561.3.2020)**

2 lipca 2020 r. Prezes UODO wydał decyzję nakładającą na Głównego Geodetę Kraju administracyjną karę pieniężną w wysokości 100 000 zł.

Adresat decyzji naruszył art. 31 RODO oraz art. 58 ust. 1 lit. e i f RODO poprzez niezapewnienie Prezesowi UODO w trakcie kontroli dostępu do pomieszczeń, sprzętu i środków służących do przetwarzania danych osobowych oraz dostępu do danych osobowych i informacji niezbędnych organowi nadzorczemu do realizacji jego zadań, jak również poprzez brak współpracy w trakcie tej kontroli.

Nakładając administracyjną karę pieniężną, Prezes UODO wziął pod uwagę, że:
- uzasadnienie odmowy wyrażenia zgody na przeprowadzenie kontroli przetwarzania przez Głównego Geodetę Kraju danych osobowych nie zasługiwało na akceptację organu nadzorczego;
- odmowa wyrażenia zgody na przeprowadzenie kontroli w zakresie określonym w punktach 1–5 upoważnień imiennych uniemożliwiła w pełnym zakresie przeprowadzenie czynności kontrolnych we wskazanych w nich obszarach;
- w niniejszej sprawie brak było jakiejkolwiek współpracy ze strony Głównego Geodety Kraju w zakresie przeprowadzanej kontroli.

Komentarz

Decyzje Prezesa UODO w powyższych sprawach, nakładające administracyjne kary pieniężne, świadczą o dużym znaczeniu obowiązku współpracy na podstawie art. 31 RODO. Współpraca z organem nadzorczym odgrywa istotną rolę w szczególności w przypadku:
- przeprowadzania kontroli;
- rozpatrywania skarg osób, których danych dotyczą;
- weryfikacji zgłoszenia naruszenia ochrony danych.

ARTYKUŁY I PUBLIKACJE

#czasopisma

„Obowiązek informacyjny w sektorze publicznym” - artykuł autorstwa **dr. hab. Grzegorza Sibiga** i **dr Igi Małobęckiej-Szwast**, który ukaże się w kolejnym numerze ABI Expert (lipiec – wrzesień).

„IoT w motoryzacji” – artykuł autorstwa **r.pr. Dominiki Nowak** na temat przetwarzania danych osobowych kierowców i pasażerów przez pojazdy wyposażone w elektroniczne jednostki kontrolujące i urządzenia sieciowe, który ukaże się w kolejnym numerze ABI Expert (lipiec – wrzesień).

„Spełnianie obowiązku informacyjnego w sektorze prywatnym” – artykuł autorstwa **r.pr. Dominiki Nowak** oraz **adw. Katarzyny Syski**, który ukaże się w kolejnym numerze ABI Expert (lipiec – wrzesień).

Przegląd decyzji europejskich organów nadzorczych dotyczących obowiązków administratora autorstwa **Mateusza Kupca**, który ukaże się w kolejnym numerze ABI Expert (lipiec – wrzesień).

„Nie każda kamera jest legalna” – wywiad **z dr. hab. Grzegorzem Sibiga** na temat monitoringu wizyjnego w spółdzielniach mieszkaniowych i wspólnotach, który ukazał się w Rzeczpospolitej z dnia 21 sierpnia 2020 r.

GOŚĆ NIERUCHOMOŚCI

Nie każda kamera jest legalna

Kary za nielegalny monitoring są wysokie. Mimo to wiele wspólnot i spółdzielni mieszkaniowych popełnia błędy – ostrzega Grzegorz Sibiga, adwokat, partner w Kancelarii Traple, Konarski, Podrecki i Wspólnicy.

ZESPÓŁ RODO

Xawery Konarski
Adwokat, Senior Partner
xawery.konarski@traple.pl

dr hab. Grzegorz Sibiga
Adwokat, Partner
grzegorz.sibiga@traple.pl

Katarzyna Syska
Adwokat, Senior Associate
katarzyna.syska@traple.pl

Dominika Nowak
Radca prawny, Senior Associate
dominika.nowak@traple.pl

dr Iga Małobęcka-Szwast LL.M.
Senior Associate
iga.malobecka@traple.pl

Mateusz Kupiec
Trainee
mateusz.kupiec@traple.pl