NR 5 - LIPIEC-WRZESIEŃ 2021

NEWSLETTER RODO

Temat numeru:
Transfer danych do państw trzecich

Pozostałe tematy artykułów:

- Ochrona danych osobowych a otwieranie danych i ponowne wykorzystywanie informacji sektora publicznego
- Wspólna opinia EROD i EIOD dot. unijnego projektu rozporządzenia ws. SI
- Ostateczna wersja zaleceń EROD dot. środków uzupełniających
- Transfer danych osobowych do Wielkiej Brytanii bez dodatkowych wymagań
- Kara dla Amazona w rekordowej wysokości 746 mln euro

Traple Konarski Podrecki & Wspólnicy

TKP

Ostateczna wersja zaleceń EROD dot. środków uzupełniających

dr Iga Małobęcka-Szwast

Dnia 18 czerwca 2021 r. Europejska Rada Ochrony Danych (EROD) przyjęła, po konsultacjach publicznych, ostateczną wersję Zaleceń 1/2020 dotyczących środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych (dalej: „Zalecenia"). Zalecenia mają kluczowe znaczenie dla dokonywania transferów danych do państwa trzeciego po wyroku TSUE w sprawie C-311/18 (Schrems II).

Pierwsza wersja Zaleceń została przyjęta w listopadzie 2020 r. w następstwie wyroku TSUE w sprawie Schrems II i poddana konsultacjom publicznym. O tej wersji Zaleceń pisaliśmy w numerze newslettera z listopada 2020 r.

Dokument ten w założeniu ma pomóc administratorom i podmiotom przetwarzającym dane (eksporterom danych) w ich obowiązku określenia i wdrożenia odpowiednich środków uzupełniających, jeżeli są one niezbędne do zapewnienia merytorycznie równoważnego stopnia ochrony danych przekazywanych do państw trzecich.

Ostateczna wersja Zaleceń zawiera kilka zmian w stosunku do pierwotnej wersji. Zostały one przyjęte w związku z uwagami zgłaszanymi podczas konsultacji publicznych. Do głównych zmian należą:

- podkreślenie znaczenia badania praktyki organów publicznych państw trzecich w ramach oceny prawnej dokonywanej przez eksporterów w celu ustalenia, czy ustawodawstwo lub praktyki państwa trzeciego rzutują – w praktyce – na skuteczność mechanizmu transferowego z art. 46 RODO[1];
- możliwość uwzględnienia przez eksportera w swojej ocenie m.in. praktycznego doświadczenia importera (z pewnymi zastrzeżeniami);
- wyjaśnienie, że ustawodawstwo państwa trzeciego umożliwiające jego organom dostęp do przekazywanych danych, nawet bez interwencji importera, może również wpływać na skuteczność narzędzia transferu.

Zalecenia zawierają plan działań (mapę drogową), jakie muszą podjąć eksporterzy danych, aby ustalić, czy potrzebne jest wdrożenie środków uzupełniających w celu przesyłania danych poza EOG zgodnie z prawem UE. W ostatecznej wersji Zaleceń zachowano sześcioetapowy proces oceny przedstawiony w wersji skierowanej do publicznych konsultacji.

Krok	**Wyjaśnienie**
Rozpoznanie przeprowadzanych operacji przekazywania	Rozpoznanie („zmapowanie") przeprowadzanych operacji transferowych, z uwzględnieniem wszystkich zaangażowanych podmiotów – importerów danych (tutaj w szczególności: Facebook Inc.). Należy także sprawdzić, czy dane, jakie zostaną przekazane, są adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przekazywane i przetwarzane w państwie trzecim.
Określenie wykorzystywanych narzędzi (instrumentów) transferowych	Weryfikacja wykorzystywanych instrumentów (mechanizmów) transferowych, o których mowa w rozdziale V RODO, w odniesieniu do poszczególnych operacji transferowych, zidentyfikowanych w ramach pierwszego kroku.
Ocena, czy wykorzystywane narzędzie przekazywania z art. 46 RODO jest skuteczne w świetle wszystkich okoliczności przekazywania	Przeprowadzenie oceny skuteczności zabezpieczeń wynikających z przyjętego na podstawie art. 46 RODO instrumentu transferowego, tj. sprawdzenie, czy w prawie lub praktyce państwa trzeciego funkcjonuje cokolwiek, co w kontekście danej operacji przekazywania mogłoby negatywnie wpłynąć na skuteczność odpowiednich zabezpieczeń wykorzystywanych narzędzi przekazywania. Ocena powinna skupiać się przede wszystkim na przepisach państwa trzeciego, które znajdują zastosowanie do danej

[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).

	operacji przetwarzania i do wykorzystywanego narzędzia przetwarzania z art. 46 RODO, a które może doprowadzić do zmniejszenia stopnia jego ochrony.
Przyjęcie środków uzupełniających	Jeśli ocena przeprowadzona w trzecim kroku wykazała, że wybrane narzędzie przekazywania z art. 46 RODO nie jest skuteczne, konieczne jest rozważenie, w stosownych przypadkach we współpracy z importerem danych, czy dostępne są jakiekolwiek środki uzupełniające, które po dodaniu do zabezpieczeń zawartych już w narzędziach przekazywania mogłyby zapewnić, że przekazywane dane są objęte w państwie trzecim stopniem ochrony merytorycznie równoważnym temu gwarantowanemu w UE.
Podjęcie kroków proceduralnych w przypadku, gdy zidentyfikowano skuteczne środki uzupełniające	Podjęcie wszelkich formalnych kroków proceduralnych, jakich może wymagać przyjęcie środka uzupełniającego w zależności od wykorzystywanego narzędzia przekazywania z art. 46 RODO. W szczególności jest to wystąpienie do właściwego organu nadzorczego o zezwolenie na planowany transfer danych (zgodnie z art. 46 ust. 3 RODO) oraz powiadomienie właściwego organu nadzorczego o sytuacji, w której eksporter danych ustali, że importer nie jest w stanie wywiązać się ze zobowiązań wynikających z przyjętego instrumentu transferowego, a mimo to eksporter nie rezygnuje z transferu danych.
Ponowna ocena w odpowiednich odstępach czasu	Konieczność dokonywania okresowej oceny stopnia ochrony danych przekazywanych do państw trzecich i monitorowanie, czy wystąpiły lub wystąpią jakiekolwiek zmiany w tym zakresie. Zasada rozliczalności (art. 5 ust. 2 RODO) wymaga zachowania stałej czujności w odniesieniu do stopnia ochrony danych osobowych.

Przy ocenie ryzyka transferu istotne jest m.in.:

- uwzględnienie wszystkich uczestników ekosystemu i tego, czy będzie dochodziło do dalszych transferów (*onward transfers*);
- uwzględnienie konkretnych kategorii danych, które będą przekazywane, konkretnych okoliczności przekazania oraz obowiązujących przepisów prawa i praktyki – w szczególności Zalecenia wyjaśniają, że praktyka stosowania przepisów może podważyć zabezpieczenia zapewniane przez prawo państwa docelowego lub może wykazać, iż prawo to nie jest stosowane do kategorii przekazywanych danych;
- odwoływanie się do standardów określonych w Zaleceniach EROD 02/2020 dotyczących niezbędnych gwarancji europejskich dla środków nadzoru z dnia 10 listopada 2020 r.;
- poleganie na źródłach informacji, które są istotne, obiektywne, wiarygodne, weryfikowalne i publicznie dostępne lub możliwe do oceny w inny sposób.

Zalecenia zawierają również otwarty katalog przykładowych środków uzupełniających (dodatkowych zabezpieczeń), które podzielone są na trzy rodzaje:

- **środki techniczne**, np. szyfrowanie danych (z uwzględnieniem szczegółowych wymogów określonych przez EROD), transfer danych poddanych pseudonimizacji, odpowiednie rozdzielenie danych między odrębnych importerów danych (*data splitting*, *multi-party processing*);
- **dodatkowe środki umowne**, np. wprowadzenie do umowy transferowej dodatkowych zobowiązań po stronie importera danych w związku z realizacją wniosków o dostęp do danych kierowanych przez organy publiczne państwa trzeciego;
- **środki organizacyjne**, np. dodatkowe wewnętrzne polityki importera danych, powołanie odpowiedniego zespołu do obsługi wniosków organów publicznych.

Dokument jest szczególnie istotny dla firm, które przy dokonywaniu transferu danych do państwa trzeciego polegają na standardowych klauzulach umownych, wiążących regułach korporacyjnych lub innych „odpowiednich zabezpieczeniach" z art. 46 ust. 2 RODO.

Źródło:
https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en;
https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_en.

Transfer danych osobowych do Wielkiej Brytanii bez dodatkowych wymagań

Dominika Nowak

Komisja Europejska przyjęła dwie decyzje wykonawcze stwierdzające odpowiedni poziom ochrony danych osobowych w Wielkiej Brytanii:

- decyzję wykonawczą z 28.06.2021 zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie odpowiedniej ochrony danych osobowych przez Wielką Brytanię;
- decyzję wykonawczą z 28.06.2021 zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/680 w sprawie odpowiedniej ochrony danych osobowych przez Wielką Brytanię.

Uznanie określonego państwa trzeciego za zapewniające odpowiedni poziom ochrony danych osobowych umożliwia ich swobodne przekazywanie przez podmioty z Europejskiego Obszaru Gospodarczego (EOG) bez konieczności korzystania z innych mechanizmów wymienionych w rozdziale V RODO[1].

Decyzja Komisji stwierdzająca odpowiedni poziom ochrony to mechanizm określony w art. 45 RODO.

Wyżej wskazane decyzje zapewniają taki swobodny transfer danych osobowych do Wielkiej Brytanii.

Obydwie decyzje weszły w życie 28 czerwca 2021 r. i zostały wydane na okres czteroletni, czyli będą obowiązywały do 27 czerwca 2025 r. Jeżeli w tym czasie Wielka Brytania będzie nadal zapewniać odpowiedni poziom ochrony danych osobowych, Komisja Europejska może przedłużyć obowiązywanie tych decyzji.

Wydanie decyzji przez Komisję kończy czas niepewności prawnej co do legalności przekazywania danych osobowych przez podmioty z EOG. Jednocześnie od tego momentu Wielka Brytania jest uznawana za państwo trzecie, co może oznaczać konieczność aktualizacji klauzul informacyjnych oraz dokumentacji przetwarzania danych osobowych.

Więcej informacji i treść decyzji:
https://uodo.gov.pl/pl/138/2097.

[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).

Ochrona danych osobowych a otwieranie danych i ponowne wykorzystywanie informacji sektora publicznego

dr hab. Grzegorz Sibiga, prof. INP PAN

Ponowne wykorzystywanie jest obszarem harmonizowanym przez prawo Unii Europejskiej. Przedmiotowa ustawa wdraża Dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego[1]. Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego[2] zastępuje Ustawę z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego[3], która z kolei implementowała dyrektywę 2003/98/WE[4] zmienioną dyrektywą 2013/37/UE[5]. Przyczyną formalną uchwalenia krajowej ustawy były zatem zmiany w prawie UE, które niosą ze sobą nowe zasady ponownego wykorzystywania informacji sektora publicznego (ISP) w całej Unii.

Cel i zakres stosowania nowych przepisów

Informacje sektora publicznego są ważnym materiałem wyjściowym dla dóbr, produktów i usług tworzonych w obrocie komercyjnym i niekomercyjnym, a podmioty publiczne wytwarzają, gromadzą lub przechowują ogromną ilość informacji i treści. Nowa ustawa określa zasady i tryb udostępniania i przekazywania informacji sektora publicznego w celu ponownego wykorzystywania oraz zasady otwartości danych, jak również podmioty, które udostępniają lub przekazują te informacje.

Z kolei przez pojęcie ponownego wykorzystywania rozumiemy wykorzystywanie przez użytkowników informacji sektora publicznego w jakimkolwiek celu, poza realizacją zadań publicznych przez podmioty do tego zobowiązane. Związane jest z tym przysługujące każdemu prawo do ponownego wykorzystywania ISP (prawo użytkownika), którego korelatem jest obowiązek podmiotów zobowiązanych dotyczący udostępniania (z własnej inicjatywy) lub przekazywania (na wniosek użytkownika) ISP do ponownego wykorzystywania. Podmioty zobowiązane wymieniono (wraz z wyjątkami) w art. 3 u.p.w., a są nimi głównie prawie wszystkie jednostki sektora finansów publicznych.

Przedmiotem obrotu są informacje sektora publicznego, zdefiniowane jako „każda treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będąca w posiadaniu podmiotu zobowiązanego". W ustawie wyodrębniono również szczególną kategorię ISP „otwartych danych", tj. danych mających istotne znaczenie dla rozwoju ponownego wykorzystywania, ponieważ mają one być udostępniane (przekazywane) w postaci elektronicznej, kompletne, aktualne, w wersji źródłowej, w otwartym i niezastrzeżonym formacie przeznaczonym do odczytu maszynowego, a do tego ich ponowne wykorzystywanie ma być bezpłatne na tych samych zasadach dla każdego użytkownika, bez konieczności potwierdzania przez niego tożsamości. Jednym z głównych rozwiązań przewidzianych w ustawie jest aktywizujący otwieranie danych *Program otwierania danych*, a źródłem takich danych będzie *Portal danych*; oba prowadzone przez ministra właściwego do spraw informatyzacji (obecnie: Prezes Rady Ministrów).

Ochrona danych osobowych

W przepisach nowej ustawy znajduje się kilka rodzajów przepisów odnoszących się do ochrony danych osobowych, ponieważ ISP mogą stanowić dane osobowe lub je zawierać, a

[1] Dz. Urz. UE L 172 z 26.06.2019 r.
[2] Dz. U. z 2021 r., poz. 1641 (dalej: „u.p.w.").
[3] Dz. U. z 2019 r., poz. 1446 (dalej: „ustawa z 2016 r.").
[4] Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 345 z 31.12.2003 r.).
[5] Dyrektywa 2013/37/UE Parlamentu Europejskiego i Rady z dnia 26 czerwca 2013 r. zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 175/1).

samo ponowne wykorzystywanie jest przetwarzaniem w rozumieniu art. 4 pkt 2 RODO[6]. Należy pamiętać – co tłumaczy motyw 154 RODO – że art. 86 RODO przewidujący „godzenie" (*to reconcile*) w prawie krajowym lub unijnym praw informacyjnych oraz prawa do ochrony danych osobowych w kształcie ustanowionym w RODO stosuje się także do relacji ponownego wykorzystywania ISP oraz ochrony danych osobowych.

Przepisy zawarte w u.p.w. odnoszące się do ochrony danych osobowych dotyczą:

- relacji między przepisami (tj. przepisami o ochronie danych osobowych oraz przepisami przedmiotowej ustawy);
- ograniczenia prawa do ponownego wykorzystywania ISP ze względu na ochronę danych osobowych;
- warunków ponownego wykorzystywania ISP stanowiących lub zawierających dane osobowe.

W większości nowe przepisy nawiązują do dotychczasowych rozwiązań w tym zakresie zawartych w ustawie z 2016 r., ale w porównaniu z nimi dokonano pewnych modyfikacji, jak również zrezygnowano z niektórych elementów. Dlatego w dalszej części tekstu będę się odwoływał także do przepisów ustawy z 2016 r.

Relacja między przepisami

Zgodnie z art. 7 ust. 2 u.p.w. przepisy przedmiotowej ustawy nie naruszają przepisów o ochronie danych osobowych. Z jednej strony zasada ta potwierdza, że przetwarzanie ISP będących danymi osobowymi objęte jest zakresem stosowania przepisów o ochronie danych osobowych, w tym – pomimo niewymienienia wprost tego aktu – przepisami ogólnego rozporządzenia o ochronie danych. Przepisy RODO będą miały zastosowanie w pełnym zakresie i u.p.w. nie ogranicza tego w żadnym stopniu. Z drugiej strony tak generalnie sformułowana zasada nie może być traktowana jako wystarczające „pogodzenie" praw (prawa do ponownego wykorzystywania oraz prawa do ochrony danych osobowych), co przewiduje się w art. 86 RODO.

Ograniczenie ponownego wykorzystywania danych osobowych

W art. 6 ust. 2 u.p.w. wprowadza się daleko idące ograniczenie możliwości ponownego wykorzystywania ISP będących danymi osobowymi. Zgodnie z tym przepisem prawo do ponownego wykorzystywania ISP podlega ograniczeniu ze względu na prywatność osoby fizycznej, w tym ochronę danych osobowych, a ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym informacji o warunkach powierzenia i wykonywania funkcji, ani przypadku, gdy osoba fizyczna wyrazi zgodę na przetwarzanie jej danych osobowych w celu ponownego wykorzystywania.

Ochrona danych osobowych stanowi zatem element prywatności podlegający ochronie przed ponownym wykorzystywaniem, co stanowi *novum* w stosunku do ustawy z 2016 r., w której prywatność była jedynym wymienionym w tej sferze dobrem chronionym. Ze względu na wąsko wyznaczony wyjątek we wspomnianym przepisie może jednak dojść do znaczącego ograniczenia procesu przeznaczania danych osobowych do ponownego wykorzystywania.

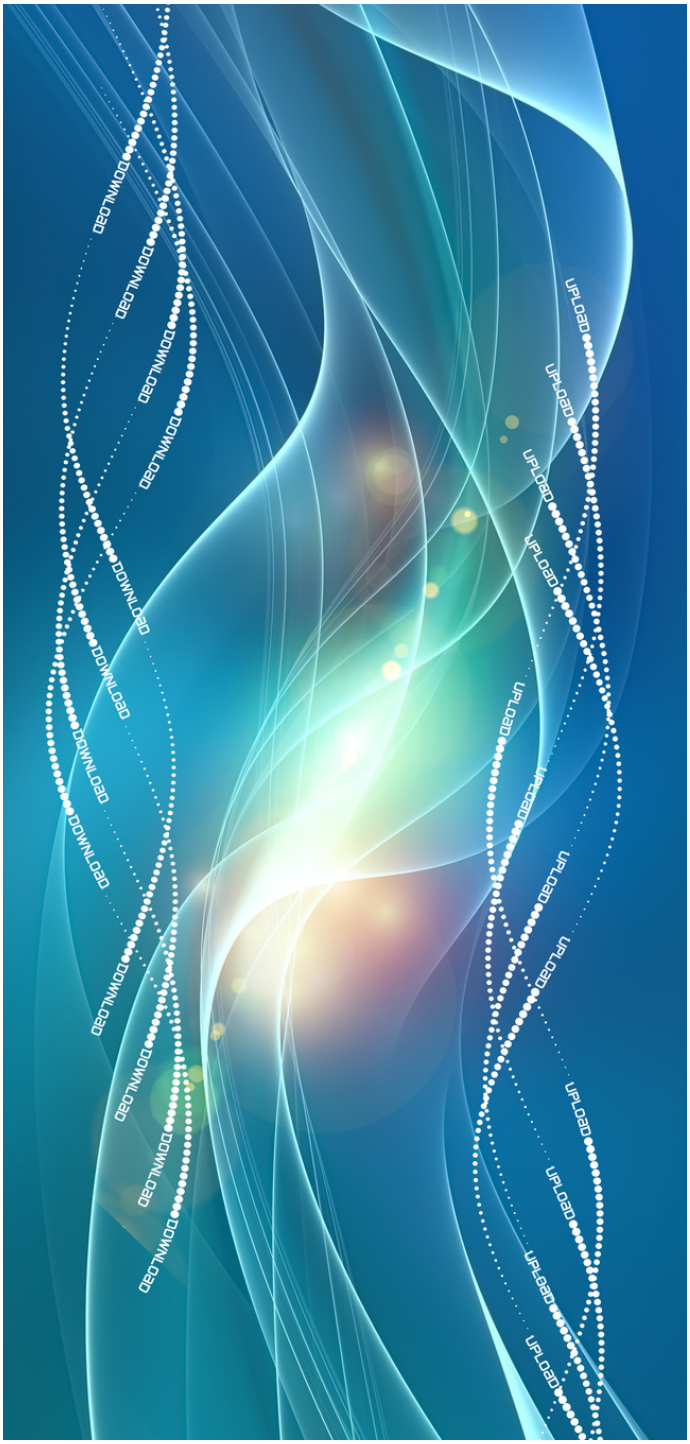
Warunki ponownego wykorzystywania

Według art. 15 ust. 1 pkt 4 u.p.w. podmiot zobowiązany może określić warunki ponownego wykorzystywania informacji sektora publicznego stanowiących lub zawierających dane osobowe. Prawie wiernie powtórzono w tym zakresie rozwiązanie z ustawy z 2016 r. Chodzi w nim o to, że w ofercie ponownego wykorzystywania podmiot zobowiązany może określić warunki dotyczące ochrony danych osobowych podlegających takiemu wykorzystywaniu. W przypadku przyjęcia tej oferty przez użytkownika (poprzez oświadczenia lub czynność pobrania ISP) następuje zawarcie umowy o ponowne wykorzystywanie ISP między podmiotem zobowiązanym oraz użytkownikiem. Wówczas warunki ochrony danych osobowych stają się obowiązkami umownymi użytkownika, o ile wcześniej zostały zawarte w ofercie przez podmiot zobowiązany.

[1] Dz. Urz. UE L 172 z 26.06.2019 r.
[2] Dz. U. z 2021 r., poz. 1641 (dalej: „u.p.w.").
[3] Dz. U. z 2019 r., poz. 1446 (dalej: „ustawa z 2016 r.").
[4] Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 345 z 31.12.2003 r.).
[5] Dyrektywa 2013/37/UE Parlamentu Europejskiego i Rady z dnia 26 czerwca 2013 r. zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 175/1).

Rezygnacja z odniesienia do art. 13 ust. 3, art. 14 i art. 19 RODO

Natomiast w porównaniu z ustawą z 2016 r. w przepisach u.p.w. rezygnuje się ze szczegółowego odniesienia do praw osób, których dane dotyczą, i obowiązków administratorów określonych w art. 13 ust. 3, art. 14 i art. 19 RODO. Od momentu wejścia w życie nowej ustawy realizacja tych uprawnień i obowiązków będzie się odbywała wyłącznie na podstawie przepisów RODO. To o tyle istotne, że ustawa z 2016 r. przewidywała wyłączenie stosowania art. 13 ust. 3 oraz art. 14 ust. 1–4 RODO w przypadku ponownego wykorzystywania ISP, natomiast realizacja uprawnienia z art. 19 RODO następowała w ten sposób, że podmiot zobowiązany aktualizował dane odpowiednio na swojej stronie podmiotowej Biuletynu Informacji Publicznej, w centralnym repozytorium lub w inny sposób.



Dla użytkowników ISP kluczowy pozostawał art. 7 ust. 4 ustawy z 2016 r., zgodnie z którym:

„Do przetwarzania przez użytkownika, w celu ponownego wykorzystywania, danych osobowych:

1. osób pełniących funkcje publiczne mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania tych funkcji,
2. osób fizycznych reprezentujących osoby prawne, w tym ich dane kontaktowe,
3. obejmujących nazwę (firmę), numer identyfikacji podatkowej (NIP) albo imię i nazwisko kontrahenta podmiotu zobowiązanego.

– przepisów art. 14 ust. 1–4 RODO nie stosuje się”.

W nowej ustawie to zwolnienie nie występuje, co oznacza potrzebę wykonania wobec podmiotów danych, których dane osobowe się ponownie wykorzystuje, obowiązku informacyjnego na warunkach określonych w art. 14 RODO.

Z całością ustawy można zapoznać się tutaj:
http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210001641.

Wspólna opinia EROD i EIOD nr 5/2021 dotycząca unijnego projektu rozporządzenia ws. sztucznej inteligencji

Mateusz Kupiec

Opublikowany w kwietniu bieżącego roku przez Komisję Europejską projekt unijnego rozporządzenia ws. sztucznej inteligencji (Artificial Intelligence Act) stanowi pierwszą próbę stworzenia kompleksowych ram prawnych dla zautomatyzowanych, samouczących się rozwiązań. W czerwcowym wydaniu newslettera zespołu RODO kancelarii przedstawialiśmy najważniejsze elementy proponowanego aktu prawnego. W tym numerze przyglądamy się stanowisku dwóch najważniejszych unijnych organów nadzorczych z zakresu ochrony danych osobowych: Europejskiego Inspektora Ochrony Danych (EIOD) i Europejskiej Rady Ochrony Danych (EROD) na temat projektu rozporządzenia. Oba organy wydały niedawno wspólną opinię, w której przedstawiają swoje uwagi dla unijnego prawodawcy w zakresie regulacji sztucznej inteligencji w UE. Przekazujemy wybrane ustalenia EIOD i EROD dotyczące projektu rozporządzenia.

Podejście oparte na ryzyku i systemy sztucznej inteligencji wysokiego ryzyka

- EIOD i EROD pozytywnie oceniają przyjęcie przez unijnego prawodawcę **podejścia opartego na ryzyku** jako głównej zasady projektowanego aktu prawnego. Niemniej oba organy stoją na stanowisku, że zasada ta powinna zostać dookreślona na etapie dalszych prac legislacyjnych, a związane z nią pojęcie „zagrożenia dla praw i wolności" – dostosowane do sposobu, w jaki jest ono rozumiane w świetle RODO.
- W ocenie organów w projekcie rozporządzenia za mało uwagi poświęca się osobom, których dotyczą działania systemu sztucznej inteligencji. W tym kontekście autorzy opinii sugerują europejskiemu prawodawcy wyraźne uwzględnienie w ostatecznej wersji rozporządzenia środków ochrony prawnej dostępnych dla osób fizycznych, na które wpływ wywarły systemy sztucznej inteligencji.
- EROD i EIOD zwracają także uwagę, że wprowadzenie w projekcie rozporządzenia zamkniętej listy systemów sztucznej inteligencji wysokiego ryzyka w formie załączników może podważyć kluczowe dla tego aktu prawnego podejście oparte na ryzyku. EROD i EIOD podkreślają, że lista systemów wysokiego ryzyka będzie musiała być regularnie aktualizowana, aby jej zakres odpowiadał rzeczywistym uwarunkowaniom społecznym i technologicznym. Ponadto oba organy spostrzegają, że klasyfikowanie systemu sztucznej inteligencji jako systemu wysokiego ryzyka nie zawsze oznacza, że jest on sam w sobie zgodny z prawem i jako taki może być wdrożony przez inny podmiot (użytkownika).
- W opinii podkreśla się, że dostawcy systemów sztucznej inteligencji nie zawsze będą w stanie przeprowadzić wymaganą ocenę ryzyka dla wszystkich przypadków wykorzystania oferowanego przez nich systemu sztucznej inteligencji. Zdaniem organów przeprowadzenie pełnej oceny ryzyka wymaga również uwzględnienia charakterystyki technicznej danego rozwiązania oraz konkretnych przypadków jego zastosowania.

Zakazane wykorzystanie systemów sztucznej inteligencji

- EIOD i EROD wzywają unijnego prawodawcę do wprowadzenia ogólnego zakazu wykorzystywania wszelkiego rodzaju systemów sztucznej inteligencji do rozpoznawania cech ludzkich (np. twarz, chód) w publicznie dostępnych przestrzeniach w jakimkolwiek zakresie.
- Organy uznają wprowadzenie wyjątków od generalnego zakazu używania systemów biometrycznej identyfikacji w miejscach publicznych za wadliwe samo w sobie, ponieważ takie podejście może sprzyjać powstawaniu nadużyć.

- EIOD i EROD stoją na stanowisku, że wykorzystanie sztucznej inteligencji do wnioskowania o emocjach osoby fizycznej jest wysoce niepożądane i powinno być zabronione, z wyjątkiem pewnych ściśle określonych przypadków użycia, mianowicie do celów zdrowotnych lub badawczych, przy zachowaniu odpowiednich zabezpieczeń i przestrzeganiu wymogów prawnych.

Certyfikacja i kodeksy postępowań

- W zakresie zaproponowanego mechanizmu certyfikacji systemów sztucznej inteligencji organy zauważają, że w projekcie brakuje wyraźnego odniesienia do prawa ochrony danych oraz innych unijnych i krajowych przepisów mających zastosowanie do każdego obszaru systemów sztucznej inteligencji wysokiego ryzyka, wymienionych w załączniku III do projektu rozporządzenia. Zdaniem EROD i EIOD w szczególności unijny prawodawca powinien uwzględnić zasady minimalizacji danych i ochrony danych jako jeden z aspektów, które należy wziąć pod uwagę przed uzyskaniem certyfikatu przez konkretny system.
- Odnośnie do przepisów rozporządzenia dotyczących kodeksów postępowania EIOD i EROD wskazują, że należy wzmocnić konstrukcję tych instrumentów poprzez wprowadzenie mechanizmów monitorowania przestrzegania kodeksów postępowania, mających na celu sprawdzenie, czy dostawcy systemów AI niezwiązanych z wysokim ryzykiem przestrzegają ich postanowień. Brak obowiązku uwzględnienia w kodeksie mechanizmu monitorowania jego przestrzegania może bowiem osłabić skuteczność kodeksu jako instrumentu zapewniającego zgodność działania systemu sztucznej inteligencji z unijnymi przepisami.

Komentarz

Jako że sztuczna inteligencja jest nierzadko wykorzystywana jako narzędzie służące do ingerowania w autonomię informacyjną jednostki (np. systemy rozpoznawania twarzy, systemy podejmujące decyzje o jednostce na podstawie profilowania, bez udziału czynnika ludzkiego), a dane osobowe są wykorzystywane jako materiał szkoleniowy dla algorytmów opartych na uczeniu maszynowym, można się spodziewać, że projekt rozporządzenia ws. sztucznej inteligencji będzie jeszcze wielokrotnie analizowany przez unijne i krajowe instytucje zajmujące się ochroną prywatności osób fizycznych. Wspólna opinia EROD i EIOD pokazuje, że najważniejsze unijne organy dążą do jak największej ochrony osób fizycznych, które będą obcować z systemami sztucznej inteligencji.

Ze wspólną opinią EROD i EIOD na temat rozporządzenia ws. sztucznej inteligencji można zapoznać się pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en.

EROD przyjmuje wiążącą decyzję w sprawie WhatsApp Ireland Ltd. na podstawie art. 65 RODO

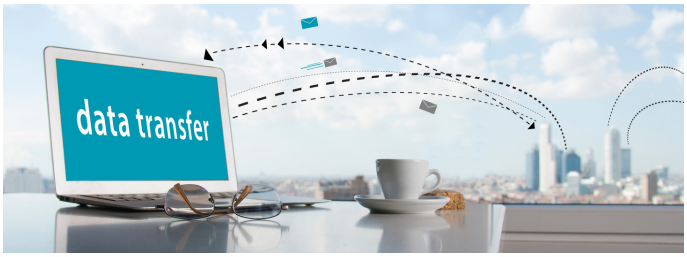
dr Iga Małobęcka-Szwast

Podczas 53. posiedzenia plenarnego, które odbyło się 28 lipca 2021 r., Europejska Rada Ochrony Danych (EROD) przyjęła decyzję rozstrzygającą spór w sprawie WhatsApp Ireland Ltd. zgodnie z art. 65 RODO[1]. Wiążąca decyzja przyjęta przez EROD ma na celu rozwiązanie kwestii braku porozumienia w odniesieniu do niektórych aspektów projektu decyzji wydanej w tej sprawie przez irlandzki organ nadzorczy, pełniący w tym przypadku rolę organu wiodącego, oraz późniejszych sprzeciwów zgłoszonych przez inne organy nadzorcze, których sprawa dotyczy.

Stosownie do art. 65 ust. 1 lit. a RODO, aby zapewnić właściwe i spójne stosowanie niniejszego RODO, EROD przyjmuje wiążące decyzje m.in. wtedy, gdy w przypadku, o którym mowa w art. 60 ust. 4 RODO[2], organ nadzorczy, którego sprawa dotyczy, zgłosił mający znaczenie dla sprawy i uzasadniony sprzeciw wobec projektu decyzji wiodącego organu nadzorczego, a wiodący organ nadzorczy odrzucił taki sprzeciw jako niemający znaczenia dla sprawy lub nieuzasadniony. Wiążąca decyzja dotyczy wszystkich spraw, które są przedmiotem mającego znaczenie dla sprawy i uzasadnionego sprzeciwu, w szczególności zaś odnosi się do tego, czy doszło do naruszenia RODO.

W niniejszej sprawie wiodący organ nadzorczy po przeprowadzeniu postępowania wyjaśniającego w sprawie WhatsApp Ireland Ltd. sporządził projekt decyzji, która dotyczyła spełnienia obowiązków w zakresie przejrzystości zgodnie z art. 12, 13 i 14 RODO przez WhatsApp Ireland Ltd.

Dnia 24 grudnia 2020 r. wiodący organ nadzorczy, działając zgodnie z procedurą, o której mowa w art. 60 ust. 3 RODO, przedłożył projekt decyzji organom nadzorczym, których sprawa dotyczy. Organy nadzorcze, których sprawa dotyczy, zgłosiły sprzeciwy zgodnie z art. 60 ust. 4 RODO, dotyczące m.in. stwierdzonych naruszeń RODO, tego, czy konkretne dane należy uznać za dane osobowe, i konsekwencji z tym związanych, a także adekwatności przewidywanych środków naprawczych.



Po rozpatrzeniu sprzeciwów organów nadzorczych, których sprawa dotyczy, irlandzki organ nadzorczy nie był w stanie osiągnąć konsensusu, w związku z czym poinformował EROD, że nie zamierza się przychylać do zgłoszonych sprzeciwów. W konsekwencji zgodnie z art. 65 ust. 1 lit. a RODO irlandzki organ nadzorczy skierował sprawę do EROD w celu jej rozstrzygnięcia. W dniu 28 lipca 2021 r. EROD przyjęła wiążącą decyzję, która dotyczy podstaw sprzeciwów uznanych za „mające znaczenie dla sprawy i uzasadnione" w rozumieniu art. 4 pkt 24 RODO[3]. EROD zapowiedziała, że wkrótce dokona formalnej notyfikacji decyzji organom nadzorczym, których sprawa dotyczy.

Zgodnie z art. 65 ust. 6 RODO irlandzki organ nadzorczy zobowiązany będzie do przyjęcia ostatecznej decyzji względem administratora (WhatsApp Ireland Ltd.), na podstawie decyzji wydanej przez EROD, bez zbędnej zwłoki i najpóźniej miesiąc po notyfikacji decyzji przez EROD. Po notyfikacji administratorowi decyzji krajowej przez irlandzki organ nadzorczy EROD opublikuje decyzję na swojej stronie internetowej.

Źródło: https://edpb.europa.eu/news/news/2021/edpb-adopts-art-65-decision-regarding-whatsapp-ireland_pl.

[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).
[2] Art. 60 ust. 3 RODO stanowi, że: „Wiodący organ nadzorczy niezwłocznie przekazuje innym organom nadzorczym, których sprawa dotyczy, stosowne informacje dotyczące danej sprawy. Niezwłocznie przedkłada innym organom, których sprawa dotyczy, nadzorczym projekt decyzji w celu uzyskania ich opinii i należytego uwzględnienia ich uwag". „Jeżeli w terminie czterech tygodni od otrzymania wniosku o opinię zgodnie z [art. 60] ust. 3 [...] inny organ nadzorczy, którego sprawa dotyczy, zgłosi mający znaczenie dla sprawy i uzasadniony sprzeciw wobec projektu decyzji, wiodący organ nadzorczy – jeżeli nie przychyla się do mającego znaczenie dla sprawy i uzasadnionego sprzeciwu lub sądzi, że sprzeciw nie ma znaczenia dla sprawy lub nie jest uzasadniony – przekazuje sprawę w ramach mechanizmu spójności, o którym mowa w art. 63 RODO" (art. 60 ust. 4 RODO).
[3] „Mający znaczenie dla sprawy i uzasadniony sprzeciw" oznacza sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia niniejszego rozporządzenia lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z niniejszym rozporządzeniem, który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii.

Wytyczne Konferencji Niezależnych Organów Ochrony Danych Federacji i Krajów Związkowych (DSK) w sprawie przekazywania danych osobowych za pomocą wiadomości e-mail

Mateusz Kupiec

Podmioty biorące udział w obrocie danymi mają obowiązek zapewnienia bezpieczeństwa informacjom, które przetwarzają. W związku z popularyzacją pracy zdalnej w organizacjach przekazuje się wewnętrznie lub na zewnątrz coraz więcej informacji za pomocą wiadomości e-mail. Konferencja Niezależnych Organów Ochrony Danych Federacji i Krajów Związkowych (DSK) opublikowała wytyczne w sprawie przekazywania danych osobowych za pomocą wiadomości e-mail. Mogą być one przydatne dla administratorów i podmiotów przetwarzających w skutecznym zapewnieniu odpowiedniego poziomu bezpieczeństwa przekazywanych danych.

Uwagi ogólne DSK

- DSK wskazuje, że zarówno szyfrowanie od końca do końca (szyfrowanie *end-to-end*, E2EE), jak i szyfrowanie w standardzie Transport Layer Security (TLS) zmniejszają ryzyko związane z naruszeniem poufności przesyłanych wiadomości email. Dlatego administratorzy muszą wziąć pod uwagę oba protokoły podczas decydowania o stosowanych zabezpieczeniach przekazywanych danych.
- Zdaniem autorów wytycznych wysoki poziom ochrony poufności treści przekazywanych za pomocą wiadomości e-mail osiąga się poprzez szyfrowanie *end-to-end*, dla którego standardy internetowe S/MIME (RFC 5751) i OpenPGP (RFC 4880) są ogólnie dostępne w połączeniu z PGP/MIME (RFC 3156). Szyfrowanie typu end-to-end chroni informacje nie tylko wtedy, gdy są one „w ruchu" (przekazywane pomiędzy urządzeniami za pomocą sieci) transportu, lecz także wówczas, gdy są przechowywane na urządzeniach. Szyfrowanie typu *end-to-end* pozwala ograniczyć przetwarzanie niezaszyfrowanych treści do specjalnie chronionych segmentów sieci lub do tych jej części, które są przeznaczone wyłącznie do użytku przez upoważnione osoby.
- Stosowanie szyfrowania w standardzie TLS zapewnia jedynie podstawową ochronę i stanowi minimalny środek do spełnienia wymagań prawnych. W sytuacjach przetwarzania o zwykłym poziomie ryzyka dla praw i wolności podmiotów danych takie szyfrowanie zapewnia wystarczającą minimalizację ryzyka.
- Podmioty wysyłające dane osobowe wewnątrz organizacji lub do zewnętrznego odbiorcy za pomocą wiadomości e-mail muszą podjąć dodatkowe środki techniczne i organizacyjne, aby o wiadomości, która ma zostać wysłana, wiedział wyłącznie odbiorca. Do tego celu (zwłaszcza w przypadku przesyłania informacji, których naruszenie wiązałoby się z wysokim ryzykiem dla praw i wolności osób fizycznych) służy szyfrowanie typu *end-to-end* z indywidualnym adresowaniem do osoby, dla której treść ma być przeznaczona.

Odbieranie danych osobowych przekazywanych za pomocą wiadomości e-mail w sytuacji zwykłego ryzyka dla praw i wolności osób, których dane dotyczą

- Ochrona poufności i integralności danych osobowych podczas przesyłania wiadomości e-mail wymaga współpracy nadawcy i odbiorcy. Chociaż za pojedynczy proces przekazywania danych osobowych za pomocą wiadomości e-mail odpowiada nadawca, to każdy podmiot, który konkretnie otrzymuje dane osobowe przez pocztę elektroniczną, jest zobowiązany do stworzenia warunków bezpiecznego odbierania wiadomości e-mail za pośrednictwem szyfrowanego kanału.
- Serwer odbiorcy wiadomości musi przynajmniej umożliwiać nawiązywanie połączeń TLS (bezpośrednio przez SMTPS[1] lub po otrzymaniu polecenia STARTTLS[2] przez SMTP).
- W celu weryfikacji autentyczności i integralności otrzymanych wiadomości e-mail należy sprawdzić podpisy DKIM[3] wiadomości.

[1] Protokół komunikacji za pomocą wiadomości e-mail przez Internet.
[2] Polecenie protokołu używane do informowania serwera poczty elektronicznej, że klient poczty elektronicznej chce zmienić połączenie z niezabezpieczonego na bezpieczne przy użyciu TLS lub SSL.
[3] DKIM (DomainKeys Identified Mail) to protokół wprowadzający zaszyfrowaną sygnaturę do nagłówka wszystkich wiadomości wychodzących w celu potwierdzenia tego, że nadawcą wiadomości jest właściciel adresu.

Odbieranie danych osobowych przekazywanych za pomocą wiadomości e-mail w sytuacji wysokiego ryzyka dla praw i wolności osób, których dane dotyczą

- Jeżeli podmioty zaangażowane w obrót danymi otrzymują pocztą elektroniczną dane osobowe, w przypadku których naruszenie poufności stanowi wysokie ryzyko dla praw i wolności danych osób fizycznych, muszą wdrożyć zarówno szyfrowanie w standardzie TLS, jak i szyfrowanie w standardzie *end-to-end*.

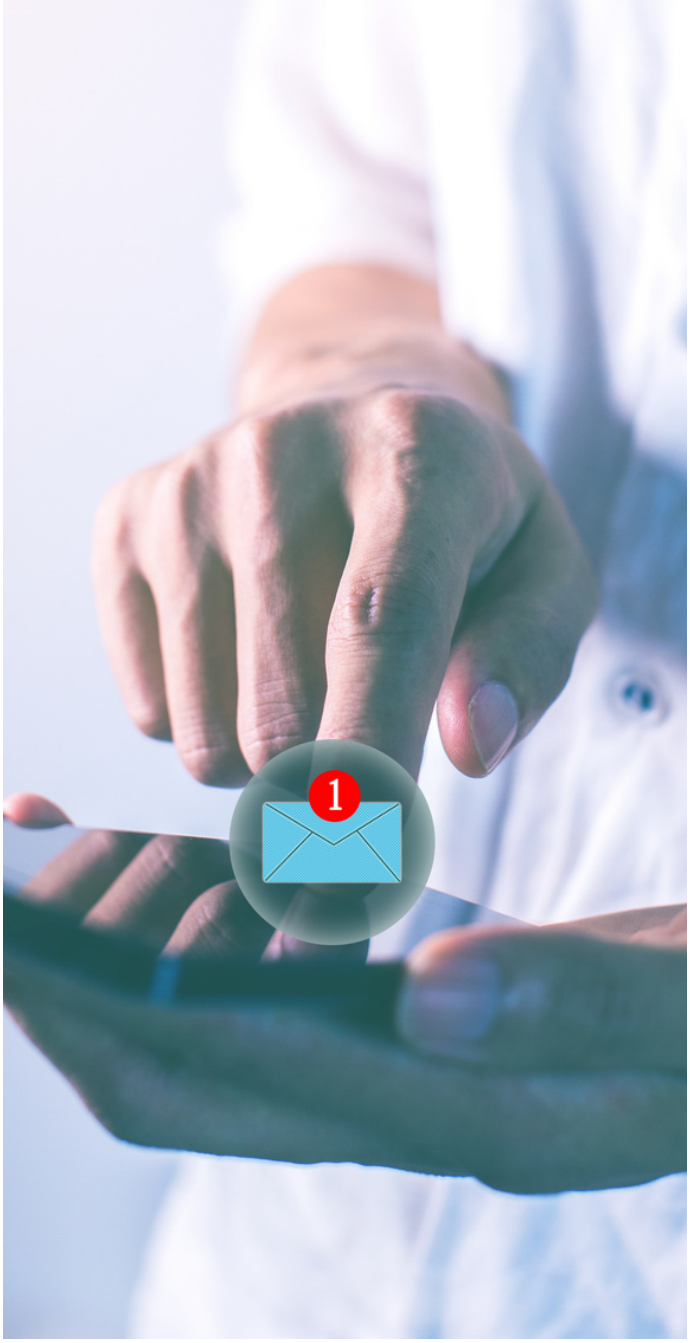
Przesyłanie danych osobowych za pomocą wiadomości e-mail w sytuacji zwykłego ryzyka dla praw i wolności osób, których dane dotyczą

- Wszyscy administratorzy wysyłający wiadomości e-mail zawierające dane osobowe, w przypadku których naruszenie poufności (treści lub okoliczności komunikatu w odniesieniu do osób fizycznych) stwarza ryzyko dla praw i wolności osób fizycznych, powinni kierować się zasadami wskazanymi w dokumencie TR 03108-1[4] i wdrożyć standard szyfrowania TLS.

Przesyłanie danych osobowych za pomocą wiadomości e-mail w sytuacji wysokiego ryzyka dla praw i wolności osób, których dane dotyczą

- Administratorzy wysyłający wiadomości e-mail zawierające dane osobowe, których naruszenie stwarzałoby wysokie ryzyko dla praw i wolności osób fizycznych, powinni co do zasady regularnie stosować szyfrowanie typu *end-to-end* i kwalifikowane szyfrowanie w standardzie TLS.

Z tekstem wytycznych DSK można zapoznać się pod adresem: https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf.



[4] *BSI TR-03108-1: Secure E-Mail Transport. Requirements for E-Mail Service Providers (EMSP)regarding a secure Transport of E-Mails*, dostępny pod adresem: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03108/TR03108-1.pdf?__blob=publicationFile&v=4 (dostęp: 12.08.2021).

Znamy treść wyroku WSA w Warszawie w sprawie skargi SGGW na decyzję PUODO

Justyna Tyburska

Stan faktyczny

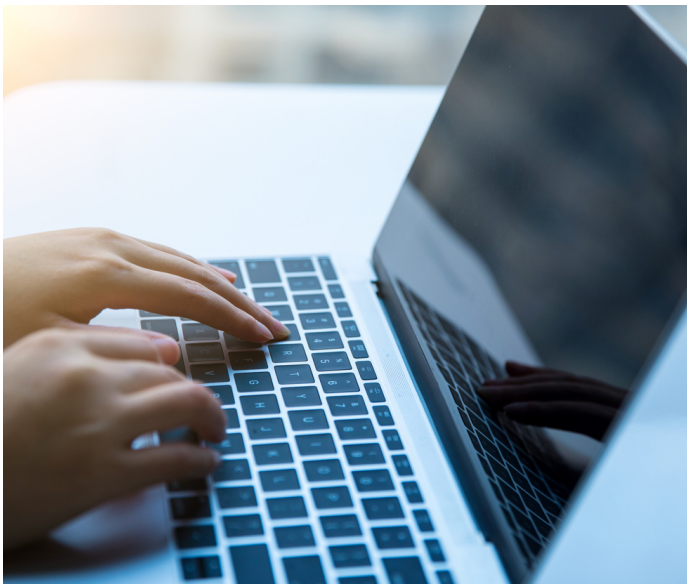
W listopadzie 2019 r. doszło do kradzieży prywatnego laptopa pracownika uczelni, na którym przechowywał dane osobowe kandydatów na studia. Zarówno kontrola, jak i postępowanie wyjaśniające UODO wykazały nieprawidłowości po stronie administratora danych. Szkoła Główna Gospodarstwa Wiejskiego w Warszawie nie dokonała analizy ani oceny ryzyka przetwarzanych danych.

Uczelnia próbowała udowodnić, że to nie ona była administratorem danych, które znajdowały się w skradzionym, prywatnym komputerze jej pracownika. Zdaniem SGGW to pracownik był administratorem danych, ponieważ bez wiedzy administratora, z naruszeniem wewnętrznych procedur, przetwarzał dane rekrutacyjne studentów z okresu pięciu lat na prywatnym sprzęcie. Uczelnia w wewnętrznych regulacjach określiła, że dane kandydatów na studia mogą być przetwarzane przez trzy miesiące od momentu zakończenia rekrutacji.

Stanowisko Sądu

Sąd zgodził się z UODO i uznał SGGW za administratora skradzionych danych. To uczelnia pełniła rolę administratora w dniu kradzieży prywatnego komputera pracownika, ponieważ decydowała o celach i sposobach przetwarzania danych osobowych kandydatów na studia. Reprezentant uczelni, któremu skradziono komputer z danymi, nie mógł samodzielnie decydować o celach ani sposobach ich przetwarzania. Czynności związane z przetwarzaniem danych wykonywał na polecenie przełożonego z uwagi na pełnione funkcje. Podkreślenia wymaga fakt, że pracownik był mocno zaangażowany w proces rekrutacji kandydatów na studia.

Sąd zwrócił także uwagę, że pracownik uczelni nie występował jako odrębny podmiot prawa. Działania pracownika można zatem uznać za działania pracodawcy, który ponosi pełną odpowiedzialność. Natomiast w stosunku do zatrudnionej osoby, która dopuściła się naruszenia obowiązków pracowniczych, ma możliwość egzekucji odpowiedzialności w formie odszkodowawczej, porządkowej lub dyscyplinarnej. Oceny stanu faktycznego przez Sąd nie zmieniło również to, że działania pracownika wykraczały poza powierzone mu obowiązki.



Sąd zgodził się ze stanowiskiem UODO, że to uczelnia naruszyła szereg zasad zawartych w RODO, m.in. zasadę integralności, zasadę poufności oraz zasadę przechowywania danych. Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem. W przypadku utraty, zniszczenia lub uszkodzenia przetwarzanych danych należy zapewnić im także poufność za pomocą odpowiednich środków technicznych lub organizacyjnych. W tym przypadku administrator nie przeprowadził analizy ryzyka ani nie ocenił, z jakimi zagrożeniami oraz konsekwencjami ma lub będzie miał do czynienia. W związku z powyższym na uczelni nie wdrożono odpowiednich środków technicznych i organizacyjnych, które zabezpieczyłyby przetwarzane dane. Należy zaznaczyć, że pracownik SGGW miał możliwość transferu danych z Systemu Obsługi Kandydatów na nośnik zewnętrzny. Proces ten nie był rejestrowany w systemie informatycznym.

Sąd zgodził się z organem nadzoru, że uczelnia nie kontrolowała we właściwy sposób procesu przetwarzania danych. Co więcej, nie weryfikowała również prawdziwości prowadzonych działań. Uczelnia, jako administrator danych, przyczyniła się do stwierdzenia nieprawidłowości i nałożenia kary pieniężnej.

Sprawozdanie z działalności Prezesa UODO w 2020 r.

Mateusz Kupiec

Prezes Urzędu Ochrony Danych Osobowych opublikował 26 sierpnia 2021 r. sprawozdanie ze swojej działalności w 2020 r. Dokument ten zawiera ważne informacje dotyczące czynności podejmowanych przez polski organ nadzorczy w zeszłym roku oraz problemów, które zwróciły jego uwagę. Przedstawiamy najbardziej interesujące naszym zdaniem fragmenty sprawozdania.

Działalność Prezesa UODO w liczbach

1. Do organu w zeszłym roku wpłynęły 6442 skargi, spośród których 2519 dotyczyło podmiotów sektora prywatnego. Ze wszystkich skarg, które trafiły do UODO, 1694 dotyczyły podmiotów sektora finansowego, ubezpieczeń i telekomunikacji.

2. Do organu w zeszłym roku wpłynęło 7507 zgłoszeń naruszeń, spośród których:

- 4661 zostało zgłoszonych przez podmioty sektora prywatnego, w tym aż 2104 naruszenia zostały zgłoszone przez podmioty z branży telekomunikacyjnej;
- 2691 zostało zgłoszonych przez podmioty sektora publicznego – naruszenia najczęściej zgłaszały jednostki samorządu terytorialnego;
- ok. 155 zostało zgłoszonych w międzynarodowym systemie informatycznym (IMI).

3. Prezes UODO został poinformowany o sytuacjach naruszających bezpieczeństwo danych przez inne podmioty niż administratorzy danych w 224 przypadkach.

4. W 2020 r. Prezes UODO wydał 1866 decyzji administracyjnych.

5. Decyzje lub postanowienia Prezesa UODO zostały zaskarżone w 112 przypadkach.

6. Prezes UODO wydał 13 decyzji administracyjnych w związku ze stwierdzeniem naruszenia ochrony danych osobowych, w których skorzystał z przysługujących mu w świetle RODO uprawnień naprawczych oraz możliwości nałożenia administracyjnej kary pieniężnej na podmiot naruszający przepisy o ochronie danych osobowych.

7. Przeprowadzono 12 kontroli przestrzegania przepisów dotyczących ochrony danych osobowych.

Wybrane problemy, którymi zajmował się Prezes UODO w 2020 r.

Prezes UODO w sprawozdaniu zwraca szczególną uwagę na następujące kwestie:

1. Przedmiotem skarg dotyczących przetwarzania wizerunku osób fizycznych za pomocą monitoringu wizyjnego przez podmioty prowadzące działalność gospodarczą była nierzadko odmowa udostępnienia osobom fizycznym kopii ich danych osobowych w postaci zarejestrowanego fragmentu nagrania. Administratorzy często (bezpodstawnie) zasłaniali się koniecznością ochrony autonomii informacyjnej osób trzecich znajdujących się na nagraniu.

2. Przedmiotem wielu skarg dotyczących podmiotów z sektora publicznego była kwestia udostępnienia (publikowania) danych osobowych na stronach internetowych Biuletynu Informacji Publicznej (BIP) np. w związku ze składanymi przez osoby fizyczne petycjami, interpelacjami. Organ wskazał, że podczas upubliczniania danych osobowych w BIP organ musi spełniać zasady przetwarzania z art. 5 RODO, w szczególności zasadę minimalizacji i ograniczonego celu.

3. W bankach, w których przeprowadzono kontrolę przestrzegania przepisów dotyczących ochrony danych osobowych, stwierdzono rozbieżne stanowiska w zakresie kopiowania dokumentów tożsamości klientów banków przy zawieraniu umów, ale procedury wewnętrzne kontrolowanych przedmiotów zawsze przewidywały możliwość zwielokrotniania takich dokumentów.

4. Zgłaszane do Prezesa UODO naruszenia ochrony danych najczęściej dotyczyły:

- wysyłania korespondencji w postaci papierowej lub elektronicznej zawierającej dane osobowe do niewłaściwego adresata (odbiorcy);
- uzyskania dostępu do danych przez nieuprawnioną osobę;
- utraty korespondencji w postaci tradycyjnej przez operatora pocztowego;
- niezamierzonego ujawnienia danych osobowych;
- utraty dokumentacji papierowej lub nośników zawierających dane osobowe.

Z całością sprawozdania można zapoznać się na stronie UODO: https://uodo.gov.pl/437.

Wystąpienie Federalnego Komisarza ds. Ochrony Danych i Wolności Informacji w sprawie prowadzenia fanpage'y na portalu Facebook przez federalne organy publiczne

Mateusz Kupiec

Rozwój mediów społecznościowych spowodował, że część organów publicznych w Niemczech zdecydowała się założyć oficjalne profile na portalu Facebook. Takie działania spotkały się z krytyką Federalnego Komisarza ds. Ochrony Danych i Wolności Informacji. Poniżej przedstawiamy główne argumenty Komisarza.

W ocenie Federalnego Komisarza ds. Ochrony Danych i Wolności Informacji (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI) prowadzenie oficjalnych profili na portalu Facebook przez federalne organy publiczne w sposób zgodny z zasadami ochrony danych osobowych nie jest obecnie możliwe. Zdaniem BfDI w celu zapewnienia legalności takich działań konieczne byłoby, aby organy publiczne prowadzące fanpage'e zawarły z Facebookiem porozumienie o współadministrowaniu danymi osobowymi, które spełniałoby wymogi art. 26 RODO[1].

Pomimo że zdaniem organów mających oficjalne profile na Facebooku taka forma komunikacji w znaczący sposób przybliża je do obywateli, BfDI zapowiedział, że od stycznia 2022 r. będzie stopniowo korzystać z uprawnień naprawczych wobec tych organów, przysługujących mu na podstawie art. 58 RODO. W związku z powyższym Komisarz zalecił organom usunięcie oficjalnych profili na Facebooku do końca bieżącego roku. BfDI przypomniał, że federalne organy muszą być wzorem do naśladowania w zakresie przestrzegania prawa o ochronie danych.

Ponadto w ocenie BfDI samo odesłanie użytkowników profili do Facebooka w zakresie informacji o sposobie przetwarzania ich danych nie jest wystarczające do spełnienia obowiązków wynikających z RODO.

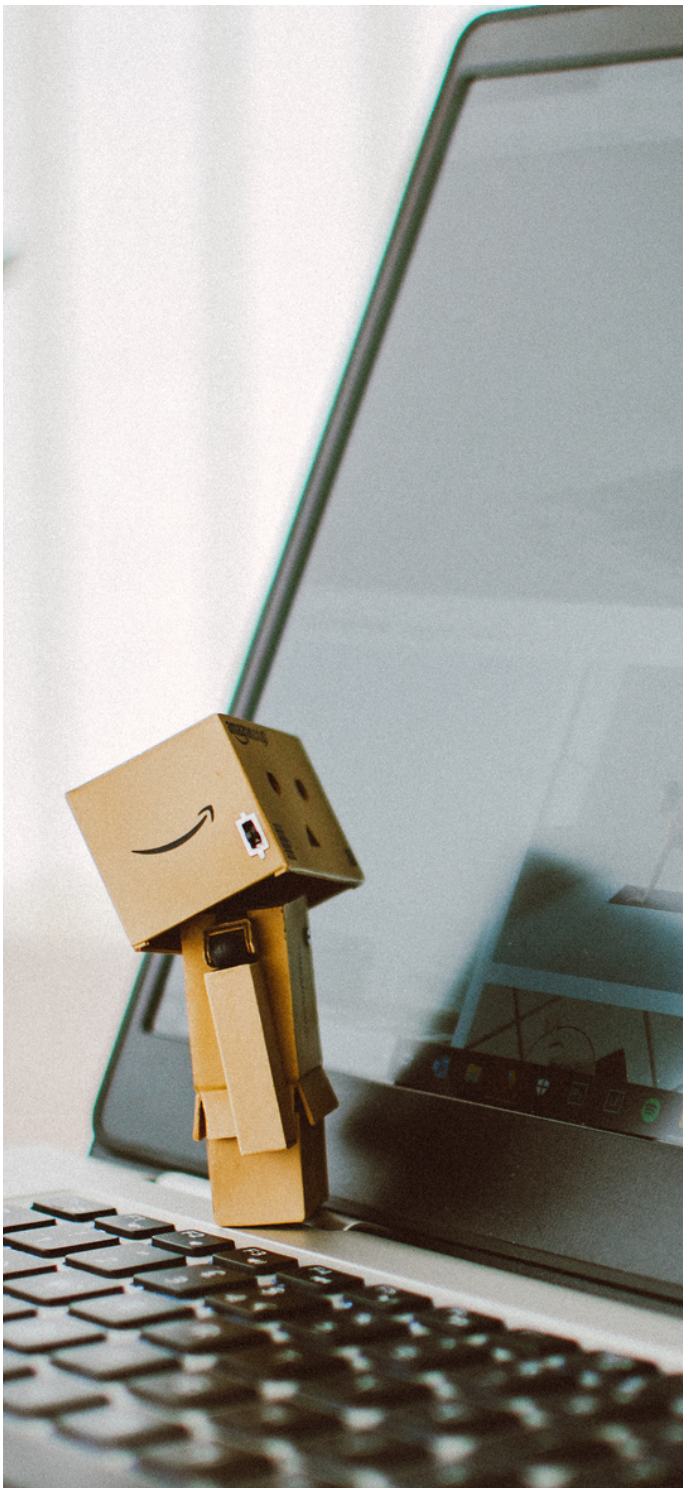
Z wystąpieniem BfDI można zapoznać się pod adresem: https://www.bfdi.bund.de/DE/DerBfDI/UeberUns/ueberuns_node.html;jsessionid=480461, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Rundschreiben/Allgemein/2021/Facebook-Auftritte-Bund.pdf?.

[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).

Kara dla Amazona w rekordowej wysokości 746 mln euro

Katarzyna Syska

Luksemburski organ nadzorczy (Commission nationale pour la protection des données; CNPD) nałożył na Amazon Europe Core S.à.r.l. karę w wysokości 746 mln euro. Naruszenia firmy dotyczą braku podstawy prawnej do przetwarzania danych do celów reklamy behawioralnej. Jest to dotychczas najwyższa administracyjna kara pieniężna nałożona na podstawie przepisów RODO.



Treść decyzji luksemburskiego organu nie jest znana, ponieważ nie publikuje on wydanych przez siebie decyzji ani nie informuje o nich publicznie.

Wiadomo jednak, że decyzja została wydana na skutek skargi francuskiej organizacji pozarządowej zajmującej się ochroną prywatności, La Quadrature du Net, reprezentującej ponad 10 tys. osób – użytkowników Amazona. Skarga została złożona 28 maja 2018 r., a zatem postępowanie w tej sprawie trwało ponad 3 lata.

W skardze zarzucono, że przetwarzanie przez Amazon danych osobowych do celów analizy behawioralnej użytkowników i wyświetlania reklamy targetowanej nie ma podstawy prawnej.

Z doniesień medialnych wynika, że decyzja luksemburskiego organu nadzorczego dotyczy właśnie przetwarzania danych w celach związanych z reklamą behawioralną (targetowaną). Regulator nakazał Amazonowi także zmianę niektórych praktyk związanych z przetwarzaniem danych osobowych.

Skarga została wniesiona do francuskiego organu nadzorczego i przekazana do luksemburskiego regulatora zgodnie z procedurą one stop shop, ponieważ spółki z grupy Amazon będące administratorami danych osobowych przetwarzanych w ramach platformy Amazon w UE mają siedziby w Luksemburgu. Amazon wskazał, że nie zgadza się z tą decyzją, i zapowiedział odwołanie się od niej.

Całkowity roczny światowy obrót Amazona w 2020 r. wynosił ok. 386 mld dolarów. W związku z tym nałożona kara wynosi ok. 0,23% całkowitego rocznego światowego obrotu za zeszły rok obrotowy (a maksymalnie mogłaby wynosić 4%).

Kara PUODO dla Prezesa Sądu Rejonowego w Zgierzu

Justyna Tyburska

Stan faktyczny

W lutym 2020 r. Prezes Urzędu Ochrony Danych Osobowych (PUODO) otrzymał zgłoszenie naruszenia ochrony danych osobowych 400 osób. Na przenośnym nośniku znajdowały się takie dane, jak: imię, nazwisko, data urodzenia, adres zamieszkania lub pobytu, numer PESEL, seria i numer dowodu osobistego, numer telefonu, informacje dotyczące wyroków skazujących, zarobków i/lub posiadanego majątku oraz zdrowia.

Mając na uwadze ryzyko naruszenia praw lub wolności osób fizycznych, administrator opublikował na stronie internetowej Sądu Rejonowego w Zgierzu komunikat dla poszkodowanych osób fizycznych, których dane dotyczą.

Decyzja organu

Postępowanie wyjaśniające organu nadzorczego wykazało, że administrator naruszył m.in. zasadę poufności i integralności danych osobowych. Należy zauważyć, że do użytku służbowego wydano kuratorowi sądowemu niezabezpieczony nośnik pamięci. Co więcej, zobowiązano kuratora – we własnym zakresie – do wdrożenia zabezpieczeń szyfrujących pamięć. W związku z brakiem wprowadzenia odpowiednich środków bezpieczeństwa w prosty sposób można było zapoznać się z danymi.

Jak wskazał w wydanej decyzji organ nadzorczy, administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka.

W dniu wydania decyzji PUODO konsekwencje naruszenia przepisów RODO przez administratora danych nadal trwały. Niezabezpieczony nośnik pamięci nie został odnaleziony, co powoduje, że osoby nieuprawnione mogą mieć dostęp do znajdujących się na nim danych osobowych. Dlatego też PUODO uznał wysokie ryzyko naruszenia praw lub wolności tych osób.

Przy ustalaniu wysokości kary pieniężnej jako okoliczność łagodzącą organ uwzględnił dobrą współpracę administratora z organem nadzorczym.

W ocenie Prezesa UODO nałożona kara będzie skuteczna i spowoduje wdrożenie przez administratora odpowiednich środków technicznych i organizacyjnych, Dostateczny stopień bezpieczeństwa w przyszłości zapewni przetwarzanym danym mniejsze ryzyko naruszenia praw i wolności osób, których dane dotyczą.

Celem przypomnienia – RODO wyróżnia dwa przedziały kar pieniężnych:

- **do 10 mln euro**, a w przypadku przedsiębiorstwa – **do 2%** jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego;
- **do 20 mln euro**, a w przypadku przedsiębiorstwa – **do 4%** jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.
- **Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r., poz. 1781) przewiduje jednak mniejsze kary dla podmiotów sektora finansów publicznych**:
- jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 Ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2021 r., poz. 305), instytuty badawcze i Narodowy Bank Polski – w wysokości **do 100 tys. zł** (tj. np. szkoły, uczelnie, szpitale, ZUS, gminy, NFZ, sądy);
- jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 Ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych – w wysokości **do 10 tys. zł** (tj. np. teatry, opery, filharmonie, kina, muzea, biblioteki, domy kultury, galerie sztuki).

Sztuczna inteligencja jako element dyplomacji państwowej i narzędzie do zdobycia przewagi politycznej i gospodarczej

dr inż. Andrzej Kaczmarek

Systemy sztucznej inteligencji (ang. *artificial intelligence* – AI) odgrywają coraz większą rolę w gospodarce. Panuje powszechna zgoda, że sztuczna inteligencja będzie kształtować przyszłość. Korzystanie z technologii maszynowego uczenia się może zrewolucjonizować wiele sektorów, przekształcić biznes i rynek pracy oraz zmienić sposób prowadzenia badań. Jest to dobrze rozumiane w Europie i na całym świecie, ale poszczególne państwa podchodzą do tych zagadnień w różny sposób. Można jednak zauważyć, że wiele z nich, jak np. Chiny i USA, rozpoczęło rywalizację w badaniach nad zastosowaniem systemów sztucznej inteligencji. Państwa te bowiem zdają sobie sprawę, jaki wpływ będą miały osiągnięcia w powyższym zakresie na politykę globalną, światową równowagę sił i sposób, w jaki sztuczna inteligencja może przyczynić się do zmiany porządku polityki międzynarodowej.

W Stanach Zjednoczonych już obecnie panuje przekonanie, że sztuczna inteligencja będzie elementem definiującym potęgę geopolityczną, mającym duży wpływ na wynik rywalizacji wielkich mocarstw, w tym między USA i Chinami, oraz na światowy układ sił. W 2018 r. Kongres USA powołał Komisję Bezpieczeństwa Narodowego ds. AI. Raport końcowy ww. Komisji został opublikowany w marcu 2021 r. Przedstawił on strategię na „wygranie ery sztucznej inteligencji". W raporcie tym przewiduje się m.in., że „zastosowane zostaną systemy sztucznej inteligencji w pogoni za władzą"[1]. Prezydent Rosji Władimir Putin był jednym z pierwszych zwolenników narracji: „Sztuczna inteligencja to potęga", zauważając w 2017 r., że: „Sztuczna inteligencja to przyszłość, nie tylko dla Rosji, ale dla całej ludzkości […]. Kto stanie się liderem w tej sferze, stanie się władcą świata"[2].

Plan rozwoju AI w Chinach na 2017 r. przewiduje wyprzedzenie Zachodu w tej dziedzinie do 2025 r.[3] Europa podchodzi jednak do wyzwań w zakresie rozwoju i zastosowań sztucznej inteligencji inaczej, chociaż instytucje UE są aktywne w tym obszarze.

W kwietniu 2021 r. Komisja przedstawiła pierwszy na świecie kompleksowy plan uregulowania sztucznej inteligencji[4]. Istnieje regulacja o usługach cyfrowych, regulacja o rynkach cyfrowych, Cyfrowa Dekada – cele Europy na 2030 r., strategia bezpieczeństwa cybernetycznego, strategia dotycząca danych i wiele innych. Po wprowadzeniu ogólnego rozporządzenia o ochronie danych (GDPR), począwszy od 2018 r., UE podwaja swoją rolę globalnego ustawodawcy w zakresie technologii i chce objąć światowe przywództwo w tej dziedzinie. Nie chce jednak angażować się w politykę władzy, która coraz częściej wiąże się z AI.

W związku z powyższym zasadne wydaje się pytanie: czy UE może trzymać się z dala od tej geopolitycznej walki o władzę nad AI, zignorować retorykę i skupić się na regulacji?

Odpowiedzi starają się udzielić autorzy raportu[5] z badań zleconych przez Departament ds. Polityki Gospodarczej, Naukowej i Jakości Życia UE na prośbę specjalnej komisji ds. sztucznej inteligencji w erze cyfrowej (Artificial Intelligence in a Digital Age – AIDA)[6].

[1] US National Security Commission on Artificial Intelligence, Final Report, marzec 2021, https://reports.nscai.gov/final-report/table-of-contents/ (dostęp: 25.08.2021).
[2] J. Vincent, Putin says the nation that leads in AI 'will be the ruler of the world', The Verge, 4.08.2017, https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world (dostęp: 16.08.2021).
[3] S.-Ch. Fischer, Artificial Intelligence: China's High-Tech Ambitions, „CSS Analyses in Security Policy", luty 2018, nr 220, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse220-EN.pdf (dostęp: 25.08.2021).
[4] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, kwiecień 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 (dostęp: 16.08.2021).
[5] Raport PE na temat dyplomacji dotyczącej sztucznej inteligencji (rozwoju AI w kontekście relacji geopolitycznych), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662926/IPOL_STU(2021)662926_EN.pdf (dostęp: 25.08.2021).
[6] Artificial Intelligence in a Digital Age, https://www.eppgroup.eu/pl/jak-dzialamy/grupy-robocze/grupa-robocza-ds-wewnetrznych-i-prawnych/sztuczna-inteligencja-w-epoce-cyfrowej (dostęp: 16.08.2021).

Dlaczego Europa nie może czekać w rozwoju AI, zajmując się głównie sprawami regulacyjnymi?

Autorzy raportu „Artificial Intelligence diplomacy. Artificial Intelligence governance as a new European Union external policy tool", opracowanego na zlecenie Departamentu ds. Polityki Gospodarczej, Naukowej i Jakości Życia UE, twierdzą, że dotychczasowe podejście UE do rozwoju i wdrażania zastosowań AI może być niewskazane z dwóch powodów.

Po pierwsze dlatego, że technologia ma charakter geopolityczny. Regulacje dotyczące sztucznej inteligencji mogą wydawać się nudnym tematem dla biurokratów, ale należy mieć świadomość, że jest to pole bitwy geopolitycznej, podobnie jak walki o rozwój i przyjęcie technologii w znaczeniu bardziej ogólnym. Rozbijanie amerykańskich firm technologicznych w momencie, gdy USA walczą o supremację z Chinami, jest działaniem geopolitycznym. Wykluczenie chińskich firm telekomunikacyjnych z europejskich sieci również jest decyzją geopolityczną. Działania Europy mają konsekwencje geopolityczne, które wykraczają poza Unię. W procesie kształtowania polityki często się o tym zapomina. W opinii autorów ww. raportu kształtowanie polityki w UE jest tak złożone, że pozostaje niewiele czasu i miejsca na przewidywanie wpływu aktorów zewnętrznych. Ogólnie rzecz biorąc, według autorów raportu UE zbyt mało uwagi poświęca myśleniu o międzynarodowych efektach drugiego i trzeciego rzędu, jakie mogą przynieść zastosowania sztucznej inteligencji, co jest działaniem niewskazanym.

Po drugie zbyt mało uwagi zwraca się na to, jak wewnętrzne (nie)działania UE wpływają na jej własną siłę geopolityczną. Na przestrzeni dziejów technologia przekształciła gospodarki i społeczeństwa, dokonała redystrybucji władzy (militarnej) między państwami, wzmocniła pozycję nowych aktorów i ukształtowała stosunki międzynarodowe. Wydaje się w związku z powyższym, że UE, pomimo całej swojej przełomowej pracy w zakresie regulacji, nie w pełni dostrzegła, jak bardzo geopolityczny charakter mają dzisiejsze technologie cyfrowe, w tym sztuczna inteligencja. Jako przykład autorzy raportu podają konferencję bezpieczeństwa w Monachium w 2020 r., na której UE była postrzegana jedynie jako moderator dyskusji pomiędzy dwoma prawdziwymi potęgami: Stanami Zjednoczonymi i Chinami. Częściowo ta geopolityczna niemoc UE wynika z jej kompetencji, ale w jeszcze większym stopniu jest ona związana ze sposobem, w jaki UE postrzega samą siebie – tj. jako podmiot rynkowy, w którym „wielka polityka" (taka jak bezpieczeństwo i obrona) pozostawiona jest w rękach państw członkowskich. Jednakże państwa członkowskie nie przejęły geopolitycznej pałeczki w kwestii AI. Choć można to postrzegać jako jeden z wielu cywilizacyjnych osiągnięć Unii Europejskiej, faktem pozostaje, że mimo iż Europa może nie chcieć myśleć o geopolityce, to geopolityka z pewnością myśli o Europie.

Zatem nawet jeśli Europa nie chce przyjąć narracji o polityce władzy w zakresie AI ani przyłączyć się do retoryki o wyścigu AI, musi wziąć pod uwagę związane z nią geopolityczne implikacje. Musi rozważyć zewnętrzny wymiar swoich działań oraz sposób postępowania z sojusznikami, partnerami, krajami, które chce wspierać, oraz przeciwnikami. Innymi słowy – UE potrzebuje planu dyplomacji w zakresie AI.

W raporcie „Artificial Intelligence diplomacy" autorzy analizują, w jaki sposób AI wpływa na geopolitykę i co to oznacza dla Europy i UE. Raport rozpoczyna się od krótkiego podsumowania na temat tego, gdzie znajdujemy się obecnie jako Europa pod względem możliwości rozwoju i zastosowań AI. Następnie zagłębia się w sedno sprawy, omawiając sześć sposobów, na jakie AI mogłaby wpłynąć – lub już wpływa – na światowy układ sił i pozycję Europy w obecnym układzie. Mowa o takich elementach, jak:

1. Konkurencja USA – Chiny.
2. Autorytaryzm wspomagany sztuczną inteligencją i osłabienie demokracji.
3. Nacjonalizm w sztucznej inteligencji.
4. Wzmocnienie sektora prywatnego.
5. Sztuczna inteligencja w bezpieczeństwie i obronie.
6. Ogólna sztuczna inteligencja (ang. *artificial general intelligence* – AGI), definiowana jako inteligencja zdolna do zrozumienia lub nauczenia się każdego zadania intelektualnego, które może wykonać człowiek.

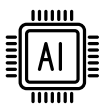
W dalszej części omówiono, czy europejskie państwa członkowskie biorą pod uwagę kwestie poruszone w ww. sześciu punktach i czy podchodzą do AI jako do tematu geopolitycznego. Dokument kończy się rekomendacjami dla UE i jej państw członkowskich, mającymi na celu zapewnienie im odpowiednich narzędzi do sprostania stojącym przed nimi wyzwaniom. Autorzy omawianego raportu kilkakrotnie odwołują się do ponad 700-stronicowego opracowania, które zostało opublikowane na początku 2021 r. przez amerykańską Komisję Bezpieczeństwa Narodowego ds. Sztucznej Inteligencji. Powołują się również na wiele innych amerykańskich opracowań, w szczególności na analizy wykonane przez Center for Security and Emerging Technologies (CSET), ośrodek badawczy na Uniwersytecie Georgetown, który został założony w 2019 r. przy wsparciu instytucji filantropijnych i amerykańskich firm technologicznych. Może to dziwić w opracowaniu dotyczącym europejskich interesów geopolitycznych i europejskich obaw o bezpieczeństwo związane z AI, ale jest to świadectwo dominacji amerykańskiego myślenia w tej przestrzeni, a także względnego braku europejskich oficjalnych publikacji w tym obszarze.

Jakie działania powinna podejmować Europa, aby sprostać wyzwaniom, jakie niesie rozwój AI?

Dominacja badań amerykańskich w zakresie AI niewątpliwie stanowi problem dla Europy. Na uwagę zasługuje fakt, że wiele analiz amerykańskich w obszarze AI dotyczy Europy (i innych sojuszników). Są to jednak badania z punktu widzenia interesów amerykańskich i jeśli Europa nie zajmie się tymi tematami z europejskiego punktu widzenia, pozostawi władzę interpretacyjną innym. Amerykański sposób myślenia będzie kształtował debatę w sposób najbardziej sprzyjający interesom USA, które nie zawsze będą idealnie zbieżne z interesami europejskimi. Dodatkowo taka dynamika stwarza ryzyko, że uwaga skupi się na tych elementach, które przede wszystkim mogą zagrozić USA, co oznacza, że istnieje niebezpieczeństwo, iż zagrożenia dla europejskich interesów i bezpieczeństwa pozostaną niedostatecznie zbadane, chyba że Europa zacznie się tym zajmować. Amerykańska społeczność zajmująca się bezpieczeństwem koncentruje się przede wszystkim na Chinach; w sprawozdaniu Komisji ds. Sztucznej Inteligencji Chiny wymieniono 699 razy, a CSET regularnie tłumaczy ważne dokumenty w języku chińskim dotyczące strategii tego państwa w zakresie sztucznej inteligencji. Natomiast inni aktorzy, tacy jak Rosja, przyciągają mniej uwagi (raport Komisji wspomina o Rosji tylko 64 razy). Tymczasem dla bezpieczeństwa europejskiego rosyjskie plany, działania i możliwości są co najmniej równie ważne. Co więcej, niektóre kwestie związane z geopolitycznymi i militarnymi zmianami siły spowodowanymi przez AI są mniej istotne dla USA, ale bardzo ważne dla Europejczyków. Na przykład wpływ, jaki systemy wojskowe oparte na AI mogą mieć na mniejsze państwa, ma dla Europejczyków kluczowe znaczenie i budzi ich zainteresowanie, zasługuje więc na znacznie więcej uwagi, a ta może zostać poświęcona jedynie w ramach badań europejskich.

Ostatecznie autorzy raportu formułują następujące zalecenia w odniesieniu do działań, jakie powinna podejmować Unia Europejska w zakresie sztucznej inteligencji:

1. UE powinna ustanowić Europejską Komisję Bezpieczeństwa ds. SI, której członkowie powinni pochodzić z różnych państw członkowskich UE, sektora prywatnego i społeczeństwa obywatelskiego. Komisja powinna przeanalizować wpływ sztucznej inteligencji na bezpieczeństwo europejskie i rozwijać zalecenia dotyczące radzenia sobie z wyzwaniami bezpieczeństwa stwarzanymi przez sztuczną inteligencję.



2. UE powinna utworzyć europejski ośrodek badawczy, który będzie się koncentrował na tych zagadnieniach związanych z SI, które mają bezpośrednie znaczenie dla Europy. Ośrodek ten mógłby służyć jako centrum dla prężnie rozwijającej się społeczności europejskich badaczy zajmujących się tymi tematami w różny sposób w państwach członkowskich. Powinien również pomagać w edukowaniu decydentów, np. poprzez krótkie szkolenia i regularne kontakty z odpowiednimi instytucjami i decydentami.

3. UE i Europejczycy powinni ściśle współpracować z USA. W opracowaniu omówiono niektóre trudności we współpracy transatlantyckiej w zakresie sztucznej inteligencji, ale zaproponowano szereg obszarów, w których UE i USA mogą ściśle ze sobą współdziałać.

4. UE powinna nadal koncentrować się na etycznej i godnej zaufania AI[7] oraz działać na rzecz jej promowania i dalszego rozpowszechniania tego podejścia w innych krajach.

5. UE powinna zachęcać państwa członkowskie do publikowania strategii rozwoju sztucznej inteligencji w zastosowaniach wojskowych, po to, aby zharmonizować różne zastosowania. Członkowie UE, którzy są członkami NATO, powinni działać w ramach NATO, aby zapewnić interoperacyjność między sojusznikami.

Wnioski

Technologia ma wymiar geopolityczny. Sztuczna inteligencja stała się elementem rywalizacji wielkich mocarstw. Jest to rzeczywistość, z którą UE i jej państwa członkowskie muszą się zmierzyć. Sztuczna inteligencja będzie miała wpływ na światową równowagę sił i stosunki między państwami, a także na geopolitykę w bardziej ogólnym ujęciu. UE musi poważnie potraktować to wyzwanie i zaangażować się w zmiany zaproponowane w omawianym dokumencie. Musi rozważyć zewnętrzny wymiar swoich działań oraz sposób postępowania z sojusznikami, partnerami, krajami, które chce wspierać, oraz przeciwnikami. W dokumencie przedstawiono przegląd możliwości UE w zakresie AI oraz omówiono sześć sposobów, na jakie AI może wpłynąć na światowy układ sił i pozycję Europy w tym układzie. Zaproponowano również sposoby, na jakie UE i jej państwa członkowskie mogą podjąć te wyzwania – czego większość państw europejskich jeszcze nie zaczęła robić. Najwyższy czas, aby Europa zainwestowała więcej czasu, wysiłku, a także pieniędzy w celu zagwarantowania, że skorzysta ona na międzynarodowych wyzwaniach, jakie niesie ze sobą AI, jednocześnie łagodząc negatywne strony tego rozwoju.

[7] *Ethics guidelines for trustworthy AI*, raport grupy ekspertów wysokiego szczebla ds. sztucznej inteligencji, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (dostęp: 28.05.2021).

PUBLIKACJE

„Przesunięcie zmian w KPA na 5.10.2021 r. nie rozwiązuje wątpliwości prawnych i dalszego prowadzenia postępowania administracyjnego na podstawie przepisów przejściowych” – opinia autorstwa dr hab. Grzegorza Sibigi, prof. INP PAN, która ukazała się na portalu Legalis.pl

Czytaj więcej

„Status prawny platform internetowych na podstawie projektu Aktu o usługach cyfrowych AUC” – artykuł autorstwa adw. Xawerego Konarskiego, który ukazał się w kwartalniku Prawo Nowych Technologii (nr 1/2021)

„Służbowa poczta poczta elektroniczna i zagrożenia z nią związane” – artykuł autorstwa r.pr. Dominiki Nowak, który ukazał się w kwartalniku ABI Expert (nr 2/2021)

„Decyzje skandynawskich organów nadzorczych” – artykuł autorstwa Mateusza Kupca, który ukazał się w kwartalniku ABI Expert (nr 2/2021)

„Sąd administracyjny po raz pierwszy zakwalifikował podmiot przetwarzający jako administratora na potrzeby określenia odpowiedzialności – konsekwencje w praktyce” – artykuł autorstwa r.pr. Dominiki Nowak, który ukazał się w kwartalniku Magazyn ODO (nr 16)

„Wyłączenie stosowania RODO do przetwarzania danych osobowych ze względu na bezpieczeństwo narodowe. Glosa do wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 6 sierpnia 2020 r., II SA/Wa 2222/19” – glosa autorstwa dr hab. Grzegorza Sibigi, prof. INP PAN, która ukazała się w czasopiśmie „Orzecznictwo Sądów Polskich” (nr 7/2021)

Czytaj więcej

„Czy algorytm może zastąpić człowieka w administracji” – artykuł autorstwa dr hab. Grzegorza Sibigi, prof. INP PAN, który ukazał się w Rzeczpospolitej

Czytaj więcej

„Amerykański fair use i japoński non-enjoyment – drogowskazy dla europejskiego prawodawcy?” - artykuł autorstwa Mateusza Kupca, który ukazał się w kwartalniku „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej” (nr 2/2021)

Czytaj więcej

„RODO II: Komunikacja w sieci, internet rzeczy, hot spoty z większą ochroną prywatności” – wywiad z adw. Xawerym Konarskim, który ukazał się w Dzienniku Gazecie Prawnej

Czytaj więcej

ZESPÓŁ RODO

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

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

dr inż. Andrzej Kaczmarek
Of counsel
andrzej.kaczmarek@traple.pl

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

Dominika Nowak
Radczyni prawna, Senior Associate
dominika.nowak@traple.pl

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

Justyna Tyburska
Junior Associate
justyna.tyburska@traple.pl

Mateusz Kupiec
Junior Associate
mateusz.kupiec@traple.pl

Redaktorzy newslettera:
dr Iga Małobęcka-Szwast
Mateusz Kupiec

Pytania prosimy kierować na adres:
rodo@traple.pl