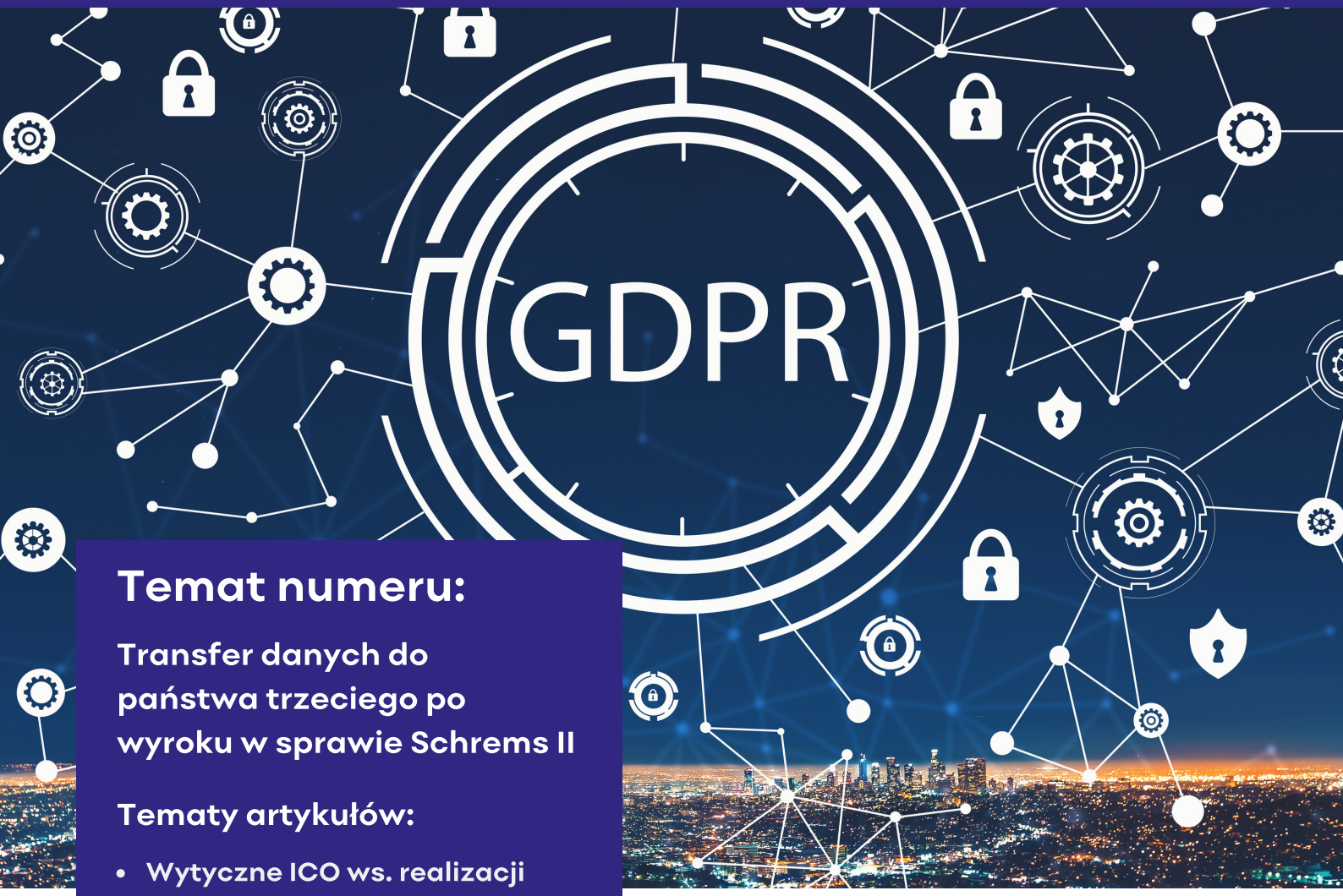
NR 5 - GRUDZIEŃ 2020

NEWSLETTER
RODO



Temat numeru:

Transfer danych do państwa trzeciego po wyroku w sprawie Schrems II

Tematy artykułów:

- Wytyczne ICO ws. realizacji żądań dostępu do danych
- Wytyczne DSK w sprawie systemów wideokonferencji
- Zgoda na przetwarzanie danych osobowych w świetle wyroku TSUE w sprawie Orange România SA
- Najnowsze naruszenia ochrony danych

Traple
Konarski
Podrecki
& Wspólnicy

TKP

Szanowni Państwo,

przedstawiamy kolejne wydanie newslettera RODO. Tematem numeru uczyniliśmy aktualny stan działań właściwych organów unijnych (rekomendacje, strategie i projekty standardów) dotyczący transferu danych do państwa trzeciego po wyroku TSUE z dnia 16 lipca 2020 r. w sprawie Schrems II ([1]

W tym przełomowym wyroku TSUE z jednej strony stwierdził nieważność decyzji Komisji Europejskiej (KE) 2016/1250 w sprawie adekwatności ochrony zapewnianej danym osobowym przekazywanym do USA przez Tarczę Prywatności UE–USA, a z drugiej strony potwierdził ważność decyzji KE 2010/87/UE zmienionej następnie decyzją Komisji nr 2016/2297 w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom w państwach trzecich. TSUE podkreślił jednak, że stosowanie standardowych klauzul umownych może się okazać niewystarczającym mechanizmem transferowym, w szczególności gdy ustawodawstwo państwa trzeciego nie zapewnia stopnia ochrony danych osobowych merytorycznie równoważnego temu, który jest gwarantowany przez przepisy RODO.

Jednocześnie z wyroku wynika, że eksporterzy danych zobowiązani są do dokonania indywidualnej oceny stopnia ochrony danych zapewnianego w ramach takiego transgranicznego przekazywania danych. Ocena ta musi uwzględniać nie tylko same postanowienia umowne uzgodnione między eksporterami i importerami danych, lecz także ustawodawstwo państwa trzeciego, w szczególności regulujące dostęp organów publicznych tego państwa do przekazywanych danych.

Co istotne, choć wyrok odnosił się wprost do transferów danych do Stanów Zjednoczonych, to ustalenia TSUE mają również zastosowanie do wszystkich odpowiednich zabezpieczeń (mechanizmów transferowych) na mocy art. 46 RODO stosowanych do przekazywania danych z EOG do dowolnego państwa trzeciego.
Od chwili wydania powyższego wyroku przez TSUE dla administratorów nie jest jasne, w jaki sposób mają dokonywać takiej oceny i jak mają zapewnić legalność transferów danych do państwa trzeciego (w szczególności do Stanów Zjednoczonych). Wychodząc naprzeciw tym wątpliwościom, w newsletterze omawiamy:

1. Rekomendacje EROD 01/2020 dotyczące dodatkowych zabezpieczeń transferu danych, które mają zapewnić poziom ochrony równorzędny z unijnym.
2. Rekomendacje EROD 02/2020 w zakresie europejskich gwarancji podstawowych dotyczących środków nadzoru.
3. Projekt standardowych klauzul ochrony danych przygotowanych przez Komisję Europejską.
4. Strategię Europejskiego Inspektora Ochrony Danych dla instytucji, urzędów, organów i agencji Unii w celu wykonania wyroku TSUE w sprawie Schrems II.

Mamy nadzieję, że nasze artykuły pomogą czytelnikom w wykonaniu niełatwego zadania, jakim jest wdrożenie ustaleń TSUE z wyroku w sprawie Schrems II i zagwarantowanie dalszego zgodnego z prawem przekazywania danych do państw trzecich.

Zapraszamy do lektury!

Redaktor newslettera: dr Iga Małobęcka-Szwast

[1] Wyrok TSUE z dnia 16 lipca 2020 r. w sprawie C-311/18 Data Protection Commissioner przeciwko Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559 (dalej: „wyrok w sprawie Schrems II").

TRANSFER DANYCH DO PAŃSTWA TRZECIEGO PO WYROKU W SPRAWIE SCHREMS II

EROD przyjęła rekomendacje w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności ze stopniem ochrony danych osobowych w UE

adw. dr hab. Grzegorz Sibiga, Partner
r.pr. Dominika Nowak, Senior Associate

Podczas 41. posiedzenia plenarnego Europejska Rady Ochrony Danych (EROD) przyjęła rekomendacje 1/2020 dotyczące środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności ze stopniem ochrony danych osobowych UE. Rekomendacje mają na celu pomóc eksporterom danych w ocenie państwa trzeciego oraz zidentyfikowaniu dodatkowych środków, które należy zaimplementować w celu zapewnienia adekwatnego poziomu ochrony. Rekomendacje zostały sformułowane w postaci mapy drogowej składającej się z sześciu elementów, które zostały opisane w tym artykule.

Wstęp

Rekomendacje EROD składają się z następujących części:

- mapa drogowa określająca poszczególne kroki, które powinni wykonać eksporterzy danych w celu oceny, czy poziom ochrony danych w państwie trzecim jest adekwatny;
- definicje wykorzystywane w rekomendacjach (załącznik nr 1);
- lista przykładowych środków technicznych, kontraktowych i organizacyjnych (załącznik nr 2);
- lista potencjalnych źródeł informacji służących do oceny adekwatności ochrony danych osobowych w państwie trzecim (załącznik nr 3).

Mapa drogowa

Mapa drogowa składa się z następujących kroków:

- Krok 1 – Poznaj swoje transfery;
- Krok 2 – Zweryfikuj narzędzia transferowe, na których opierasz przekazywanie danych;
- Krok 3 – Oceń, czy w prawie lub praktyce państwa trzeciego istnieje cokolwiek, co może mieć wpływ na skuteczność odpowiednich zabezpieczeń;
- Krok 4 – Zidentyfikuj i przyjmij środki uzupełniające;
- Krok 5 – Podejmij wszelkie formalne kroki proceduralne, których może wymagać przyjęcie środka uzupełniającego;
- Krok 6 – Ponownie oceń w odpowiednich odstępach czasu stopień ochrony danych, które przekazujesz do państwa trzeciego, oraz monitoruj, czy nastąpiły zmiany, które mogą wpłynąć na stopień ochrony.

Krok 1

W ramach pierwszego kroku należy zidentyfikować wszystkie przypadki przekazywania danych osobowych do państw trzecich w organizacji. Rejestrowanie i identyfikowanie wszystkich operacji przekazywania może być zadaniem złożonym dla podmiotów, które są zaangażowane w liczne, zróżnicowane i regularne operacje przekazywania danych. Jednak wiedza o tym, dokąd trafiają dane osobowe, jest konieczna, aby zapewnić wszędzie równoważny poziom ochrony. Przy identyfikacji operacji przetwarzania można oprzeć się na prowadzonym rejestrze czynności, rejestrze kategorii czynności z art. 30 ust. 1 i 2 RODO oraz stosowanych klauzulach informacyjnych zawierających elementy określone w art. 13 ust. 1 lit. f oraz art. 14 ust. 1 lit. f RODO. Należy także zweryfikować, czy przekazywane dane są adekwatne, stosowne oraz ograniczone do tego, co jest niezbędne do celów, w których są przekazywane.

[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).

Należy pamiętać, że zdalny dostęp do danych z państwa trzeciego lub przechowywanie danych w chmurze znajdującej się poza EOG są również uznawane za przekazywanie.

Krok 2

W ramach kroku drugiego należy dokonać weryfikacji wykorzystywanych przez eksportera danych mechanizmów przekazywania, które znajdują się w rozdziale V RODO. Jeśli Komisja Europejska stwierdziła, że dane państwo trzecie bądź jego część, region lub sektor zapewnia adekwatny poziom ochrony na podstawie decyzji stwierdzającej odpowiedni poziom ochrony wydanej na gruncie art. 45 ust. 1 RODO lub jeszcze dyrektywy 95/46, to tak długo, jak ta decyzja obowiązuje, nie ma konieczności podejmowania dalszych kroków poza monitorowaniem, czy dana decyzja pozostaje ważna. Lista decyzji Komisji Europejskiej jest publikowana na stronie internetowej [2] .

W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony należy polegać na jednym z mechanizmów transferowych określonych w art. 46 RODO, jeżeli przekazywanie danych odbywa się systematycznie i powtarzalnie. Głównymi rodzajami narzędzi przekazywania danych z art. 46 RODO są:

- standardowe klauzule ochrony danych (SCC);
- wiążące reguły korporacyjne;
- kodeksy postępowania;
- mechanizmy certyfikacji;
- klauzule umowne ad hoc.

Narzędzia określone w art. 46 RODO zawierają odpowiednie zabezpieczenia o charakterze umownym, które można stosować w celu przekazywania danych do państwa trzeciego. Należy przy tym pamiętać, że sytuacja w państwie trzecim może wymagać uzupełnienia tych narzędzi oraz zawartych tam zabezpieczeń o dodatkowe środki w celu zapewnienia merytorycznie równoważnego stopnia ochrony.

W przypadku sporadycznego i niepowtarzalnego przekazywania danych można polegać na wyjątkach określonych w art. 49 RODO. Wyjątki te należy jednak interpretować w sposób restrykcyjny.

Krok 3

W trzecim kroku należy ocenić, czy w prawie lub praktyce państwa trzeciego istnieją jakiekolwiek czynniki , które mogą mieć wpływ na skuteczność odpowiednich zabezpieczeń w odniesieniu do konkretnego przekazywania. Ocena powinna się skupiać na przepisach państwa trzeciego, które są istotne dla przekazywania danych, oraz na wykorzystywanej podstawie przekazywania danych z art. 46 RODO. Należy wziąć pod uwagę przepisy państwa trzeciego dotyczące dostępu organów publicznych do danych do celów nadzoru oraz zapoznać się z rekomendacjami EROD dotyczącymi niezbędnych gwarancji europejskich. Jeżeli w danym państwie trzecim brakuje przepisów dotyczących uzyskiwania dostępu do danych przez organy publiczne, to należy przeanalizować obiektywne czynniki, które mogą wystąpić w tym zakresie. W analizie trzeba wziąć pod uwagę wszystkie biorące udział w przekazywaniu danych podmioty (administratorów, podmioty przetwarzające oraz dalsze podmioty przetwarzające), które zidentyfikowano w kroku pierwszym.

Ramy prawne mające zastosowanie będą zależały od okoliczności przekazywania, w szczególności od:

- celów, dla których dane są przekazywane i przetwarzane;
- rodzajów podmiotów zaangażowanych w przetwarzanie (publiczne/prywatne; administrator/podmiot przetwarzający);
- sektora, w którym następuje przekazywanie (np. sektor adtech, telekomunikacja, finanse itp.);
- kategorii przekazywanych danych osobowych (np. dane osobowe dotyczące dzieci mogą wchodzić w zakres szczególnego ustawodawstwa państwa trzeciego);
- tego, czy dane będą przechowywane w państwie trzecim lub czy istnieje tylko zdalny dostęp do danych przechowywanych w UE/EOG;

[2] Zob. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_pl (dostęp: 7.12.2020).

- formatu przekazywanych danych (tj. w prostym/spseudonimizowanym lub zaszyfrowanym tekście);
- możliwości dalszego przekazywania danych z państwa trzeciego do innego państwa trzeciego.

Ocena może ostatecznie wykazać, że mechanizm przekazywania z art. 46 RODO, na którym opiera się eksporter, oraz odpowiednie zabezpieczenia w nim zawarte:

- skutecznie zapewniają, aby przekazywane dane osobowe były chronione w państwie trzecim w stopniu merytorycznie równoważnym temu gwarantowanemu w EOG;
- nie zapewniają skutecznie merytorycznie równoważnego stopnia ochrony – w takiej sytuacji obowiązkiem podmiotu przekazującego dane jest wprowadzenie skutecznych środków uzupełniających lub nieprzekazywanie danych osobowych.

Krok 4

W ramach kroku czwartego należy zidentyfikować i przyjąć środki uzupełniające niezbędne, aby stopień ochrony danych przekazywanych do państwa trzeciego był równoważny stopniowi ochrony w EOG. Ten krok jest konieczny, jeżeli ocena z kroku trzeciego wykaże, że przepisy państwa trzeciego mają wpływ na skuteczność narzędzia transferowe-go z art. 46 RODO, z którego korzysta lub zamierza korzystać eksporter danych.

Rekomendacje zawierają załącznik nr 2 obejmujący listę przykładowych dodatkowych środków wraz z niektórymi warunkami, które należy spełnić, aby te środki były skuteczne. Środki uzupełniające mogą mieć charakter umowny, techniczny lub organizacyjny. Przy ich doborze należy wziąć pod uwagę: format przekazywanych danych, charakter danych, długość i złożoność procesu przetwarzania danych, liczbę podmiotów zaangażowanych oraz możliwość dalszego przekazywania danych w tym samym państwie trzecim lub w innych państwach trzecich.

W pewnych sytuacjach może być konieczne zastosowanie więcej niż jednego dodatkowego środka. Poszczególne dodatkowe środki mogą być skuteczne w jednym państwie trzecim, ale w innym nie. Jeżeli żadne środki dodatkowe nie są w stanie zapewnić adekwatnego poziomu ochrony, to należy unikać przekazywania danych, zawiesić lub zakończyć transfer danych. Analiza dodatkowych środków powinna zostać udokumentowana zgodnie z zasadą rozliczalności.

Krok 5

W ramach kroku piątego należy podjąć wszelkie formalne działania proceduralne, które są wymagane w celu przyjęcia środka uzupełniającego, w zależności od tego, który z mechanizmów transferu z art. 46 RODO ma zostać wykorzystany.

W niektórych przypadkach może być konieczne skonsultowanie się z właściwymi organami nadzorczymi.

Krok 6

W ramach kroku szóstego należy dokonywać ponownej oceny oraz monitorować stopień ochrony danych osobowych w odpowiednich odstępach czasu pod kątem ewentualnych zmian. Ma w tym zakresie zastosowanie zasada rozliczalności, która jest obowiązkiem o charakterze ciągłym. Wprowadzone mechanizmy powinny być stabilne i zapewniać szybkie zawieszenie lub zakończenie danych, jeżeli podmiot odbierający dane naruszył zobowiązania, które podjął w ramach mechanizmu transferowego z art. 46 RODO, lub nie jest w stanie wykonywać tych zobowiązań, lub jeżeli przyjęte środki uzupełniające nie są już skuteczne.

Do 21 grudnia 2020 r. EROD prowadzi konsultacje publiczne w sprawie tych rekomendacji.

Uwagi można zgłaszać poprzez formularz:
https://edpb.europa.eu/our-work-tools/publicconsultations-art-704/reply-form?node=1102.

Tekst rekomendacji dostępny jest pod adresem (wyłącznie w języku angielskim):
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

Tłumaczenie nieoficjalne rekomendacji i załącznika nr 1 na język polski dostępne jest pod adresem:
https://uodo.gov.pl/pl/138/1774.

Komentarz

Z jednej strony rekomendacje EROD wydają się najważniejszym i najbardziej rozbudowanym po wyroku Schrems II urzędowym stanowiskiem, w którym wskazuje się eksporterom danych z krajów UE sposób zapewnienia legalności transferu danych do państw trzecich. W dokumencie porządkuje się przesłanki legalności transferu wynikające z RODO oraz określa się kolejność ich zastosowania. Przedstawia się istotne dla eksporterów wskazówki co do oceny przepisów państwa trzeciego ważnych dla przekazywania danych oraz doboru środków zabezpieczających transfer.

Z drugiej strony jednak rekomendacje nadal nie zapewniają, że skorzystanie z określonych rozwiązań daje pewność legalności transferu, a przed wyrokiem Schrems II gwarantowały to mechanizmy z art. 46 RODO. Rekomendacje w kluczowych elementach przewidują, że to na eksporterze spoczywa ciężar oceny przepisów prawa państwa importera oraz doboru środków zabezpieczających transfer. Dlatego też uzasadnione jest oczekiwanie na dalsze działania prawotwórcze i regulacyjne, które zagwarantują pewne i jednoznaczne podstawy prawne transferów do państw trzecich.

Projekt nowych standardowych klauzul umownych jako mechanizmu transferu danych do państwa trzeciego

adw. Xawery Konarski, Starszy Partner

Jak wykazuje praktyka, ponad 90% transferów danych osobowych do państwa trzeciego jest obecnie realizowanych na podstawie standardowych klauzul umownych (dalej: „SKU"), określonych w art. 46 ust. 2 lit. c RODO[1]. Znaczenie tego mechanizmu transferowego wzrosło zwłaszcza po wyroku w sprawie Schrems II, w którym zakwestionowano dopuszczalność przekazywania danych osobowych do Stanów Zjednoczonych na podstawie tzw. Tarczy Prywatności. Szczególnie istotne są więc prowadzone obecnie przez Komisję Europejską konsultacje dotyczące nowych standardowych klauzul umownych, których projekt został opublikowany 12 listopada 2020 r.

Co nowego?

Opracowanie projektu nowych standardowych klauzul służyło realizacji trzech podstawowych celów.

Po pierwsze, obecnie już obowiązujące zestawy postanowień administrator – administrator oraz administrator – podmiot przetwarzający dostosowano do wymogów określonych w RODO. Jest to tym istotniejsze, że zestawy te zostały zatwierdzone przez Komisję Europejską odpowiednio w 2004 r. i 2010 r. W ramach działań dostosowawczych m.in. wprowadzono postanowienia ujęte w art. 28 RODO, dotyczące sytuacji powierzenia przetwarzania danych osobowych.

Po drugie, w projekcie standardowych klauzul uwzględniono szereg postulatów, wyrażonych w wyroku w sprawie Schrems II, dotyczących konieczności wprowadzenia przez eksportera danych dodatkowych zabezpieczeń. Chodzi tu m.in. o środki w zakresie bezpieczeństwa danych.

Po trzecie, w projekcie nowych standardowych klauzul uwzględniono dwa scenariusze transferów danych, nieobjęte do tej pory zestawami zatwierdzonymi w 2004 r. i 2010 r. Są to odpowiednio sytuacje przekazywania danych w relacjach: podmiot przetwarzający – administrator oraz podmiot przetwarzający – podmiot przetwarzający. W ten sposób wypełniono istotną lukę, od lat już dostrzeganą przez eksporterów i importerów danych uczestniczących w przekazywaniu danych osobowych poza Europejski Obszar Gospodarczy.

Okres dostosowawczy

W projekcie standardowych klauzul przewidziano roczny okres, liczony od daty wejścia w życie nowej decyzji Komisji Europejskiej, na dostosowanie przez eksporterów i importerów danych dotychczas obowiązujących SKU do ich nowej wersji. Warunkiem jest, że dotychczasowe postanowienia pozostaną w tym okresie niezmienione, z wyjątkiem niezbędnych środków uzupełniających wprowadzonych w celu zagwarantowania, iż przekazanie danych osobowych podlega odpowiednim zabezpieczeniom w rozumieniu art. 46 ust. 1 RODO.

Dalsze prace

Konsultacje projektu standardowych klauzul umownych trwają do 10 grudnia 2020 r. Prace nad nimi są skorelowane z innymi inicjatywami podejmowanymi przez Komisję Europejską i Europejską Radę Ochrony Danych (EROD). Chodzi tu w szczególności o również obecnie konsultowane: projekt Komisji Europejskiej dotyczący standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi z siedzibą w UE oraz projekt rekomendacji EROD pt. „Rekomendacje 1/2020 w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności z unijnym poziomem ochrony danych osobowych".

Źródło: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.

[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).

EROD przyjęła rekomendacje w zakresie europejskich gwarancji podstawowych dotyczących środków nadzoru

dr Iga Małobęcka-Szwast, Senior Associate

Podczas 41. posiedzenia plenarnego Europejska Rady Ochrony Danych (EROD) przyjęła Rekomendacje 2/2020 w zakresie europejskich gwarancji podstawowych (European Essential Guarantees) dotyczących środków nadzoru. Dokument jest uzupełnieniem Rekomendacji 1/2020 dotyczących dodatkowych środków ochrony danych w przypadku transferu danych do państwa trzeciego po wyroku TSUE w sprawie Schrems II. Rekomendacje te mają w założeniu pomóc eksporterom danych w ustaleniu, czy ramy prawne regulujące dostęp organów publicznych do danych do celów nadzoru w państwach trzecich można uznać za uzasadnioną ingerencję w prawo do prywatności i ochrony danych osobowych, a zatem czy te ramy prawne nie naruszają zobowiązań wynikających z narzędzia transferowego z art. 46 RODO[1], z którego korzysta eksporter i importer danych.

Wstęp

W następstwie wyroku TSUE w sprawie Schrems II eksporterzy danych, którzy opierają się na mechanizmach transferowych, o których mowa w art. 46 RODO (w tym na standardowych klauzulach umownych), są zobowiązani do weryfikacji w każdym indywidualnym przypadku, we współpracy z odbiorcą danych w państwie trzecim, czy prawo państwa trzeciego zapewnia stopień ochrony przekazywanych danych osobowych, który jest zasadniczo równoważny z poziomem gwarantowanym w EOG.

Aby wspomóc eksporterów danych w dokonaniu tej oceny, EROD przyjął Rekomendacje 2/2020 w zakresie europejskich gwarancji podstawowych, które zastąpiły wcześniejszy dokument Grupy Roboczej Art. 29[2] przyjęty po wyroku w sprawie Schrems I[3].

EROD, opierając się na orzecznictwie TSUE, określił europejskie gwarancje podstawowe (European Essential Guarantees), których należy przestrzegać, aby zagwarantować, że ingerencja w prawo do prywatności i ochrony danych osobowych poprzez stosowanie środków nadzoru podczas transferu danych osobowych do państwa trzeciego nie wykracza poza to, co jest konieczne i proporcjonalne w demokratycznym społeczeństwie.

EROD zdecydował się zaktualizować wcześniejszy dokument, pierwotnie opracowany w odpowiedzi na wyrok w sprawie Schrems I, i rozwinąć europejskie gwarancje podstawowe, tak aby uwzględniały one późniejsze orzecznictwo TSUE i Europejskiego Trybunału Praw Człowieka (ETPC), w szczególności wyrok TSUE w sprawie Schrems II.

Europejskie gwarancje podstawowe opierają się na orzecznictwie TSUE dotyczącym art. 7, 8, 47 i 52 Karty praw podstawowych (KPP) oraz orzecznictwie ETPC na gruncie art. 8 Europejskiej Konwencji Praw Człowieka (EKPC), dotyczącym kwestii nadzoru w państwach będących stronami EKPC.

Zgodnie z Rekomendacjami 1/2020 dotyczącymi dodatkowych środków ochrony dokonanie oceny systemu prawnego państwa trzeciego w zakresie dostępu organów nadzoru do danych osobowych jest jednocześnie jednym z sześciu kroków, które powinni podjąć eksporterzy danych, decydując się na ich transfer do państwa trzeciego.

[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] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) – WP 237.
[3] Wyrok TSUE z dnia 6 października 2015 r. w sprawie C 362/14 Maximillian Schrems przeciwko Data Protection Commissioner, ECLI:EU:C:2015:650.

EROD zdecydował się zaktualizować wcześniejszy dokument, pierwotnie opracowany w odpowiedzi na wyrok w sprawie Schrems I, i rozwinąć europejskie gwarancje podstawowe, tak aby uwzględniały one późniejsze orzecznictwo TSUE i Europejskiego Trybunału Praw Człowieka (ETPC), w szczególności wyrok TSUE w sprawie Schrems II.

Europejskie gwarancje podstawowe opierają się na orzecznictwie TSUE dotyczącym art. 7, 8, 47 i 52 Karty praw podstawowych (KPP) oraz orzecznictwie ETPC na gruncie art. 8 Europejskiej Konwencji Praw Człowieka (EKPC), dotyczącym kwestii nadzoru w państwach będących stronami EKPC.

Zgodnie z Rekomendacjami 1/2020 dotyczącymi dodatkowych środków ochrony dokonanie oceny systemu prawnego państwa trzeciego w zakresie dostępu organów nadzoru do danych osobowych jest jednocześnie jednym z sześciu kroków, które powinni podjąć eksporterzy danych, decydując się na ich transfer do państwa trzeciego.

Cel europejskich gwarancji podstawowych

Celem zaktualizowanych europejskich gwarancji podstawowych jest dostarczenie wskazówek i kryteriów dla eksporterów danych, mających pomóc im w zbadaniu, czy środki nadzoru umożliwiające dostęp do danych osobowych organom publicznym w państwie trzecim, będącym krajowymi agencjami bezpieczeństwa lub organami ścigania, można uznać za uzasadnioną ingerencję w prawa podstawowe osób, których dane dotyczą, czy też nie.

Europejskie gwarancje podstawowe stanowią część oceny, którą eksporter danych powinien przeprowadzić w celu ustalenia, czy państwo trzecie zapewnia poziom ochrony zasadniczo równoważny z poziomem ochrony gwarantowanej w UE (EOG). Nie mają one jednak na celu zdefiniowania wszystkich elementów, które są konieczne do uznania, że państwo trzecie zapewnia taki poziom ochrony zgodnie z art. 45 RODO. Podobnie gwarancje te nie mają na celu same w sobie określenia wszystkich elementów, które należy rozważyć przy ocenie, czy reżim prawny państwa trzeciego uniemożliwia podmiotowi przekazującemu i odbierającemu dane zapewnienie odpowiednich zabezpieczeń zgodnie z art. 46 RODO (tj. wykaz tych elementów nie jest wyczerpujący).

Rekomendacje przedstawiają podstawowe gwarancje, jakie powinno zapewniać państwo trzecie, i w założeniu mają one pomóc w ocenie ingerencji, jaką pociągają za sobą środki nadzoru przewidziane w prawie państwa trzeciego, w zakresie prawa do prywatności i ochrony danych osobowych.

Cztery europejskie gwarancje podstawowe

Po przeanalizowaniu orzecznictwa TSUE i ETPC EROD sformułowała cztery europejskie gwarancje podstawowe, które muszą być zapewnione w państwie trzecim w kontekście stosowania przez organy publiczne środków nadzoru. Gwarancje te określają:

- w jaki sposób należy dokonywać oceny stopnia ingerencji w podstawowe prawo do prywatności i ochrony danych w kontekście środków nadzoru stosowanych przez organy publiczne w państwie trzecim przy przekazywaniu danych osobowych;
- jakie wymogi prawne muszą zostać spełnione, aby uznać, że taka ingerencja jest dopuszczalna na gruncie KPP.

EROD wskazała na następujące gwarancje:

1. Przetwarzanie powinno opierać się na jasnych, precyzyjnych i łatwo dostępnych zasadach.
2. Należy wykazać konieczność i proporcjonalność w odniesieniu do uzasadnionych celów, do których osiągnięcia zmierza dany środek nadzoru.
3. Powinien istnieć niezależny mechanizm nadzoru nad służbami uprawnionymi do dostępu do danych.
4. Osoba fizyczna musi mieć dostęp do skutecznych środków ochrony prawnej.

W ocenie EROD jeżeli system prawny państwa trzeciego spełnia powyższe wymogi prawne, ograniczenia w zakresie ochrony danych i prawa do prywatności mogą zostać uznane za uzasadnione.

Ad 1 Przetwarzanie powinno opierać się na jasnych, precyzyjnych i łatwo dostępnych zasadach

W tym kontekście EROD podkreśliła, że możliwość ingerencji organów publicznych w prawo do prywatności i ochrony danych jednostki, tj. możliwość przetwarzania przez takie organy danych osobowych, musi wynikać z przepisów prawa, które jasno i precyzyjnie wskazują, w jakich okolicznościach i na jakich warunkach może dochodzić do takiej ingerencji (przetwarzania). Taka ingerencja w prawa podstawowe musi być również przewidywalna dla jednostki co do skutków, tak aby zapewnić jej odpowiednią i skuteczną ochronę przed arbitralną ingerencją i ryzykiem nadużyć. W rezultacie przetwarzanie musi opierać się na precyzyjnej, jasnej, a także dostępnej (tj. publicznej) podstawie prawnej.

Ad 2 Konieczność i proporcjonalność w odniesieniu do uzasadnionych celów, do których osiągnięcia zmierza dany środek

W tym zakresie EROD przywołała art. 52 KPP, zgodnie z którym wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w KPP muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

W odniesieniu do zasady proporcjonalności EROD wskazuje za orzecznictwem TSUE, że kwestię, czy ograniczenie prawa do prywatności i ochrony danych można uzasadnić, należy oceniać z jednej strony poprzez ważenie stopnia ingerencji wynikającego z takiego ograniczenia, a z drugiej poprzez sprawdzenie, czy cel w interesie publicznym, któremu służy to ograniczenie, jest proporcjonalny do danego stopnia ingerencji.

Co się tyczy natomiast zasady konieczności, TSUE w wyroku w sprawie Schrems I wyjaśnił, że „uregulowanie umożliwiające generalnie przechowywanie wszelkich danych osobowych wszystkich osób fizycznych, których dane zostały przekazane z Unii (...) bez jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od zamierzonego celu i bez przewidzenia obiektywnych kryteriów, które pozwoliłyby na ograniczenie dostępu władz publicznych do danych oraz na ich późniejsze wykorzystanie do określonych celów, ściśle ograniczonych, które mogą uzasadnić ingerencję, jaką stanowi zarówno dostęp, jak i wykorzystanie tych danych" jest niezgodne z tą zasadą. W szczególności uregulowanie pozwalające władzom publicznym na uzyskanie powszechnego dostępu do treści wiadomości elektronicznych należy uznać za naruszenie zasadniczej istoty prawa podstawowego do poszanowania życia prywatnego.

Ad 3 Niezależny mechanizm nadzoru

EROD zwraca uwagę, że zgodnie z utrwalonym orzecznictwem TSUE i ETPC każda ingerencja w prawo do prywatności i ochrony danych powinna podlegać skutecznemu, niezależnemu i bezstronnemu systemowi nadzoru, który musi być zapewniony albo przez sędziego, albo przez inny niezależny organ (np. organ administracyjny lub organ parlamentarny).

Ad 4 Zapewnienie skutecznych środków ochrony prawnej dla osób, których dane dotyczą

Jak podkreślił TSUE w wyroku w sprawie Schrems II, przy ocenie adekwatności poziomu ochrony państwa trzeciego należy wziąć pod uwagę, czy osoby, których dane dotyczą, mają możliwość skorzystania przed niezawisłym i bezstronnym sądem ze środków prawnych w celu uzyskania dostępu do dotyczących tych osób danych osobowych, sprostowania lub usunięcia takich danych.

W tym kontekście TSUE uważa, że skuteczną ochronę sądową przed takimi ingerencjami może zapewnić nie tylko sąd, lecz także niezależny organ, który zapewnia gwarancje zasadniczo równoważne z gwarancjami wymaganymi na mocy art. 47 KPP (prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu). TSUE podkreślił, że należy zapewnić niezależność sądu lub organu, w szczególności od władzy wykonawczej, m.in. poprzez wprowadzenie niezbędnych gwarancji niezależności w zakresie warunków odwołania lub powołania takiego organu. Taki organ powinien być uprawniony do podejmowania decyzji, które są wiążące dla służb wywiadowczych, zgodnie z gwarancjami prawnymi, na które mogłyby się powołać osoby, których dane dotyczą.

EROD podkreślił, że powyższe cztery europejskie gwarancje podstawowe należy postrzegać jako podstawowe elementy, które należy wziąć pod uwagę przy ocenie stopnia ingerencji w podstawowe prawo do prywatności i ochrony danych. Wyżej opisane wymogi są ze sobą ściśle powiązane. Z tego względu dokonując przeglądu odpowiednich przepisów dotyczących środków nadzoru, minimalnego poziomu gwarancji ochrony praw osób, których dane dotyczą, oraz środków prawnych przewidzianych przez prawo krajowe państwa trzeciego, należy oceniać realizację tych gwarancji łącznie.

Komentarz

Europejskie gwarancje podstawowe stanowią cenną wskazówkę dla eksporterów danych, którzy przekazują dane do państwa trzeciego na podstawie mechanizmów transferowych, takich jak standardowe klauzule umowne czy wiążące reguły korporacyjne, przy ocenie, czy prawo państwa trzeciego zapewnia stopień ochrony przekazywanych danych osobowych, który jest zasadniczo równoważny z poziomem gwarantowanym w EOG.

Niemniej należy zauważyć, że dokonanie takiej oceny w sposób rzetelny nie będzie łatwym zadaniem i będzie wymagało od eksporterów danych dużego zaangażowania, nakładów pracy i środków finansowych. Nie ulega wątpliwości, że taka ocena może być rzetelnie wykonana jedynie przez podmioty, które mają odpowiednią wiedzę i środki, by pozyskać i przeanalizować ustawodawstwo państw trzecich, do których przekazywane są dane osobowe. Należy także pamiętać, że powyższa ocena nie ma charakteru jednorazowego – EROD rekomenduje, by dokonywać jej w rozsądnych odstępach czasu. Przeprowadzenie takiej oceny powinno być również odpowiednio udokumentowane przez eksportera danych, zgodnie z zasadą rozliczalności. Z tego względu należy mieć nadzieję, że krajowe organy nadzorcze dostarczą w tym zakresie dalej idących wskazówek, które ułatwią eksporterom danych przeprowadzanie oceny w odniesieniu do ustawodawstwa poszczególnych państw trzecich.

Tekst rekomendacji dostępny jest pod adresem (wyłącznie w języku angielskim):
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.

Strategia EIOD dla instytucji, urzędów, organów i agencji Unii w celu wykonania wyroku TSUE w sprawie Schrems II

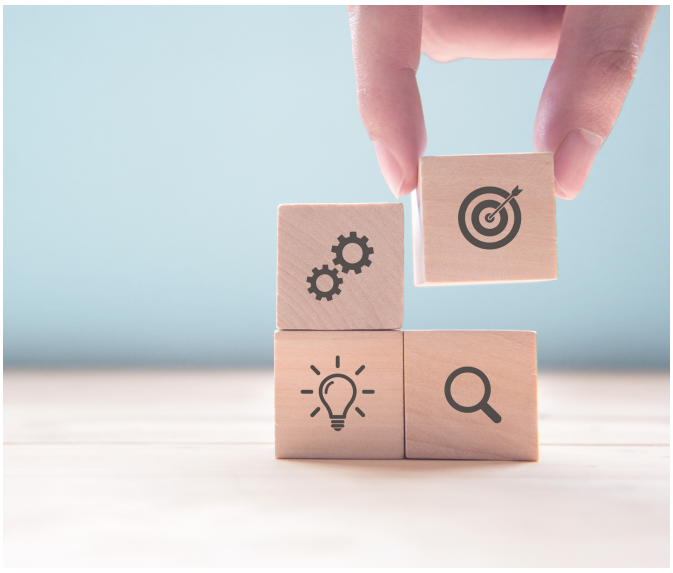
dr Iga Małobęcka-Szwast, Senior Assciate

Europejski Inspektor Ochrony Danych (EIOD) opublikował „Strategię dla instytucji, urzędów, organów i agencji Unii w celu wykonania wyroku TSUE w sprawie Schrems II". Dokument ma na celu zapewnienie, by bieżące i przyszłe transfery danych do państwa trzeciego (w szczególności do Stanów Zjednoczonych) dokonywane przez instytucje, organy, urzędy i agencje Unii Europejskiej odbywały się w sposób zgodny z Kartą praw podstawowych (KPP), a także z obowiązującymi przepisami UE dotyczącymi ochrony danych, przede wszystkim z rozporządzeniem 2018/1725[1] oraz orzecznictwem TSUE (zwłaszcza z wyrokiem w sprawie Schrems II).

Plan działania rekomendowany przez EIOD

EIOD opracował plan działania w celu zapewnienia zgodności transferów danych do państwa trzeciego z obowiązującymi przepisami prawa i wyrokiem TSUE w sprawie Schrems II. EIOD wprowadził rozróżnienie między krótkoterminowymi i średnioterminowymi działaniami w zakresie zgodności, które powinny zostać podjęte przez instytucje unijne.

W ramach **działań krótkoterminowych** na rzecz zapewnienia zgodności EIOD zalecił instytucjom unijnym, by dokonały mapowania i weryfikacji, które z bieżących umów, postępowań o udzielenie zamówienia i innych rodzajów współpracy wiążą się z transferem danych do państwa trzeciego.



Jednocześnie strategia przewiduje, że instytucje UE mają zgłaszać do EIOD transfery danych, które nie mają podstawy prawnej, transfery danych na podstawie wyjątków oraz transfery danych do podmiotów prywatnych w Stanach Zjednoczonych, które stwarzają wysokie ryzyko dla osób, których dane dotyczą. Ponadto w odniesieniu do nowych operacji przetwarzania lub nowych umów z usługodawcami EIOD rekomenduje, by instytucje UE unikały czynności przetwarzania, które obejmują przekazywanie danych osobowych do USA.

W ramach **działań średnioterminowych** EIOD zapowiedział, że będzie udzielał instytucjom unijnym wytycznych i prowadził działania w zakresie zgodności przekazywania danych do Stanów Zjednoczonych lub innych państw trzecich w indywidualnych przypadkach.

Instytucje unijne zostaną poproszone o przeprowadzenie **indywidualnych ocen skutków** transferu (transfer impact assessment) w celu ustalenia, czy w państwie trzecim zapewniony jest poziom ochrony zasadniczo równoważny z tym przewidzianym w UE (EOG). Oceny te powinny zostać przeprowadzane z pomocą importerów danych. Na podstawie tej oceny instytucje powinny podjąć decyzję, czy możliwe jest kontynuowanie transferów danych do państwa trzeciego zidentyfikowanych w ramach mapowania (działania krótkoterminowego).

Instytucje unijne zostały jednocześnie zobowiązane do składania EIOD sprawozdania na temat transferu danych na podstawie wyjątków, kontynuowanych transferów do państwa trzeciego, które nie zapewnia merytorycznie równoważnego poziomu ochrony, oraz transferów, które są zawieszone lub zakończone z powodu braku równoważnego poziomu ochrony w kraju przeznaczenia.

EIOD zapowiedział, że będzie nadal ściśle współpracował z organami nadzorczymi w ramach Europejskiej Rady Ochrony Danych (EROD), aby zapewnić spójne wdrażanie wyroku TSUE w sprawie Schrems II w EOG.

Źródło:https://edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strategy_schremsii_en_0.pdf.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE.

Pierwsza decyzja Europejskiej Rady Ochrony Danych rozstrzygająca spór na podstawie art. 65 RODO

r.pr. Dominika Nowak, Senior Associate

Dnia 9 listopada 2020 r. podczas 41. plenarnego posiedzenia Europejska Rada Ochrony Danych przyjęła pierwszą decyzję rozstrzygającą spór w trybie art. 65 RODO, która dotyczy spółki Twitter International Company. Decyzja ta jest wiążąca dla organów nadzorczych biorących udział w sporze.

Kontekst sprawy

Decyzja wydana przez Europejską Radę Ochrony Danych (EROD) dotyczy sporu powstałego w związku z:

- projektem decyzji wydanej przez irlandzki organ nadzorczy (ang. Data Protection Commission) jako wiodący organ nadzorczy (ang. leading supervisory authority; LSA) dla Twitter International Company;
- sprzeciwami zgłoszonymi przez organy nadzorcze, których sprawa dotyczy (ang. concerned supervisory authority; CSA).

Dnia 8 stycznia 2019 r. spółka Twitter International Company powiadomiła irlandzki organ nadzorczy o naruszeniu ochrony danych. W maju 2020 r. irlandzki organ nadzorczy przekazał projekt decyzji organom nadzorczym, których sprawa dotyczy, zgodnie z art. 60 ust. 3 RODO, w celu uzyskania ich opinii oraz należytego uwzględnienia ich uwag.

Następnie na podstawie art. 60 ust. 4 RODO organy nadzorcze, których sprawa dotyczy, miały cztery tygodnie na złożenie mającego znaczenie dla sprawy i uzasadnionego sprzeciwu. Organy nadzorcze, których sprawa dotyczy, złożyły sprzeciwy dotyczące naruszeń RODO stwierdzonych przez wiodący organ nadzorczy, w tym roli Twitter International Company jako jedynego administratora danych oraz kwantyfikacji proponowanej kary.

Procedura z art. 65 RODO – rozstrzyganie sporów przez EROD

Z racji tego, że wiodący organ nadzorczy odrzucił zastrzeżenia pozostałych organów nadzorczych lub uznał, że zastrzeżenia te nie są „istotne i uzasadnione", sprawa została skierowana do EROD na podstawie art. 60 ust. 4 w zw. z art. 65 ust. 1 lit. a RODO i wszczęto procedurę rozstrzygania sporu.

EROD dokonała oceny kompletności akt, a następnie dnia 8 września 2020 r. została uruchomiona procedura rozstrzygania sporów w trybie art. 65 RODO. Dnia 9 listopada 2020 r. EROD wydała wiążącą decyzję, na podstawie której irlandzki organ nadzorczy dokona ostatecznego rozstrzygnięcia. Decyzja wiodącego organu nadzorczego powinna zostać skierowana do administratora bez zbędnej zwłoki i najpóźniej miesiąc po notyfikowaniu decyzji przez EROD.

Źródło:
https://edpb.europa.eu/news/news/2020/edpb-adopts-first-art-65-decision_pl
https://edpb.europa.eu/sites/edpb/files/20201110_art65_faq.pdf

Wytyczne ICO ws. realizacji żądań dostępu do danych

adw. Katarzyna Syska, Senior Associate
Mateusz Kupiec, Trainee

W październiku 2020 r. brytyjski organ nadzorczy (Information Commissioner's Office; dalej: „ICO") opublikował wytyczne w sprawie realizacji prawa dostępu do danych. Wytyczne te skierowane są w szczególności do inspektorów ochrony danych oraz osób pełniących obowiązki w zakresie ochrony danych w organizacjach. Celem nowych wytycznych jest pomoc administratorom danych w ocenie tego rodzaju żądań. W tekście przedstawiamy wybrane elementy wytycznych.

Jak szukać danych dotyczących wnioskodawcy?

ICO przedstawia ogólne wskazówki co do tego, w jakim zakresie dane przetwarzane przez administratora powinny być przeszukiwane pod kątem wniosku o dostęp do danych. Zdaniem ICO należy dołożyć wszelkich rozsądnych starań, aby znaleźć żądane informacje. Nie ma jednak obowiązku przeprowadzać wyszukiwań, które byłyby nieproporcjonalne w stosunku do znaczenia zapewnienia dostępu do informacji.

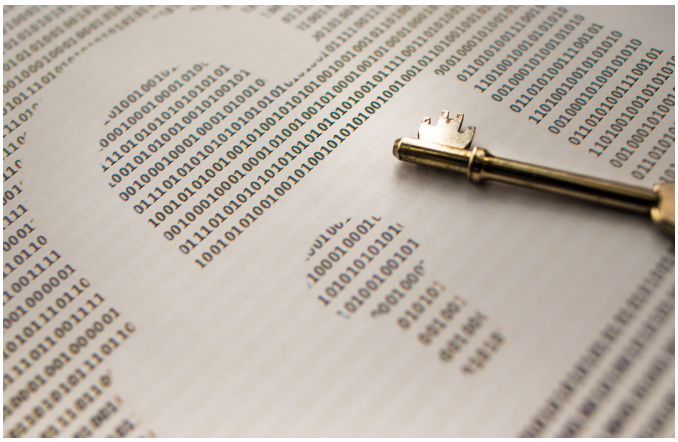
Czy trzeba przeszukiwać kopie zapasowe i archiwa?

ICO wskazuje, że konieczne jest przeszukanie archiwów oraz kopii zapasowych pod kątem tego, czy zawierają one dane osobowe wnioskodawcy. ICO przyznaje, że uzyskanie dostępu do danych zawartych w kopiach zapasowych może być skomplikowane. Jednakże w RODO nie ma żadnego wyjątku co do technologii przechowywania informacji pozwalającego na wyłączenie pewnych danych czy nośników spod prawa dostępu. Administrator powinien zatem mieć procedury wyszukiwania i odzyskiwania danych osobowych, które są zarchiwizowane w formie elektronicznej lub w kopii zapasowej.

Czy dane zawarte w e-mailach podlegają prawu dostępu?

ICO wskazuje, że prawo uzyskania dostępu do danych odnosi się także do danych osobowych zawartych w wiadomościach e-mail, a zatem konieczne jest ich odpowiednie przeszukanie pod tym kątem.

Organ zwraca uwagę, że to, czy e-mail zawiera dane osobowe konkretnej osoby, zależy od treści wiadomości e-mail, kontekstu zawartych w niej informacji i celu, w jakim jest ona używana. Może być tak, że tylko część informacji zawartych w e-mailu, który jakaś osoba otrzymała lub wysłała, stanowi jej dane osobowe. W związku z tym ICO wskazuje, że prawo dostępu ma zastosowanie wyłącznie do danych osobowych danej osoby zawartych w wiadomości e-mail. Oznacza to, że konieczne może być przekazanie jej części lub całości. Zależy to od treści e-maila i od tego, czy dotyczy on wnioskodawcy.



Czy prawo dostępu dotyczy też danych w dużych zbiorach danych?

ICO zwraca uwagę, że choć ilość i różnorodność dużych zbiorów danych (ang. big datasets) może utrudnić wypełnianie obowiązków wynikających z prawa dostępu, to jednak stosuje się je również do takich danych. RODO nie przewiduje w tym zakresie żadnego wyjątku.

Podobnie, jeśli administrator przetwarza dane z różnych źródeł danych, dane nieustrukturyzowane, dane zaobserwowane lub wywnioskowane o podmiocie danych – również co do takich danych konieczne jest spełnianie żądań dostępu.

ICO zwraca uwagę na istotność dobrego zarządzania danymi, aby ułatwić odpowiadanie na żądania dostępu do danych, a także ze względu na inne wymogi prawne RODO dotyczące rozliczalności. Konieczne jest posiadanie możliwości odpowiedniego przeszukiwania informacji w celu realizacji żądania dostępu do danych.

Jak należy postępować, jeśli żądane przez wnioskodawcę informacje obejmują dane osobowe innych osób?

ICO zauważa, że dane osobowe mogą odnosić się do więcej niż jednej osoby. Tym samym udzielenie odpowiedzi na żądanie dostępu do danych może wiązać się z udzieleniem informacji, które odnoszą się zarówno do wnioskodawcy, jak i do innej osoby. W celu zobrazowania takiej sytuacji organ posługuje się przykładem pracownika zwracającego się do pracodawcy z prośbą o kopię swojej dokumentacji pracowniczej. ICO zwraca uwagę, że taka dokumentacja może zawierać informacje identyfikujące osoby, które przyczyniły się do jej powstania.

W ocenie organu w takiej sytuacji administrator musi rozważyć, czy udostępnienie pewnych informacji nie naruszy praw i wolności osób trzecich. Wobec tego, zdaniem ICO, sporządzając odpowiedź na taki wniosek:

- administratorzy powinni przeanalizować, czy możliwe jest spełnienie żądania bez ujawniania danych osobowych osób trzecich;
- w przypadku negatywnej odpowiedzi na powyższe pytanie administratorzy powinni rozważyć zwrócenie się do osoby trzeciej z prośbą o wyrażenie zgody na przekazanie dotyczących tej osoby informacji wnioskodawcy, pod warunkiem, że jest to możliwe i nie powoduje negatywnych konsekwencji dla wnioskodawcy;
- administratorzy powinni rozważyć, czy ujawnienie informacji o osobie trzeciej jest uzasadnione pomimo braku jej zgody.

ICO wskazuje, że obowiązek zachowania poufności jest jednym z czynników, które należy wziąć pod uwagę przy podejmowaniu decyzji o ujawnieniu informacji o osobie trzeciej bez jej zgody. Niemniej administrator nie powinien zawsze zakładać istnienia takiego obowiązku w stosunku do danych osobowych osoby trzeciej.

Czy administrator może poprosić o dowód tożsamości?

Zdaniem ICO można poprosić osobę, która wnosi żądanie, o przedstawienie dowodu tożsamości, ale tylko jeśli jest to konieczne. Jednakże ICO zwraca uwagę na wymóg proporcjonalności. Jeśli tożsamość wnioskodawcy da się zweryfikować w inny sposób, to należy go zastosować. Na przykład jeśli wnioskodawca ma konto klienta w systemie administratora, to do weryfikacji tożsamości tego wnioskodawcy może posłużyć login i hasło.

Kiedy żądanie jest ewidentnie nieuzasadnione lub nadmierne?

ICO wyjaśnia też, na czym może polegać brak uzasadnienia lub nadmierność żądań.

Żądanie jest ewidentnie nieuzasadnione, jeżeli:

- wnioskujący wyraźnie nie ma zamiaru skorzystać ze swojego prawa (np. osoba składa wniosek, ale potem oferuje wycofanie go w zamian za jakąś formę korzyści od organizacji);
- żądanie jest złośliwe w zamiarze i jest wykorzystywane do nękania organizacji bez realnych celów innych niż spowodowanie zakłócenia (np. dana osoba wyraźnie oświadczyła w samym wniosku lub w innych komunikatach, że zamierza spowodować zakłócenie).

Natomiast żądanie może być nadmierne, jeśli powtarza treść poprzednich żądań, od których nie upłynął rozsądny okres, lub jeśli żądanie pokrywa się z innymi żądaniami.

Czy administrator danych osobowych może zostać zmuszony do realizacji prawa dostępu?

ICO przypomina, że organ nadzorczy w wyniku skargi wniesionej przez podmiot danych w związku z naruszeniem przepisów o ochronie danych osobowych może zobowiązać administratora danych do realizacji żądania dostępu do nich lub ustosunkowania się do żądania.

W przypadku gdy osoba fizyczna udowodni poniesienie szkody majątkowej lub niemajątkowej z powodu naruszenia praw tej osoby do ochrony danych osobowych, w tym przez niezrealizowanie jej wniosku dostępu do danych, sąd będzie mógł nakazać administratorowi wypłacenie jej odszkodowania.

Wytyczne DSK w sprawie systemów wideokonferencji

Mateusz Kupiec, Trainee

W związku z pandemią wirusa SARS-CoV-2 i koniecznością pracy zdalnej coraz więcej organizacji decyduje się używać systemów służących do przeprowadzania wideokonferencji. Zarówno dostawcy takich rozwiązań, jak i podmioty z nich korzystające muszą spełniać wymogi związane z ochroną danych osobowych. 23 października 2020 r. Konferencja Niezależnych Urzędów ds. Ochrony Danych na Poziomie Federalnym oraz Krajów Związkowych (dalej: „DSK") przyjęła wytyczne dotyczące systemów wideokonferencji, które mogą pomóc tym podmiotom spełnić obowiązki wynikające z RODO[1]. W tekście przedstawiamy wybrane zalecenia DSK.

Modele korzystania z systemów wideokonferencji

DSK wyróżnia trzy modele korzystania z systemów wideokonferencji:

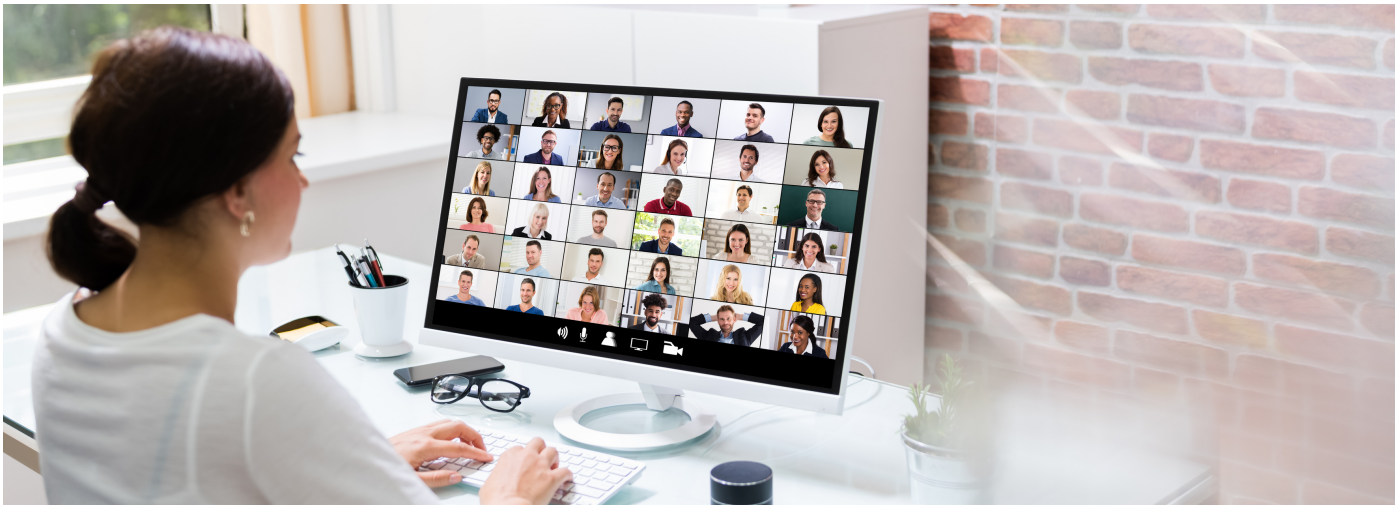
1. Samodzielna obsługa systemu wideokonferencji
Niektóre podmioty korzystają z systemów służących do przeprowadzania wideokonferencji, zainstalowanych na ich własnej infrastrukturze informatycznej. Takie rozwiązanie sprawia, że podmiot zachowuje wyłączną kontrolę nad przetwarzanymi danymi osobowymi w ramach systemu i jest jedynym administratorem danych osobowych uczestników wideokonferencji.

2. Obsługa systemu przez zewnętrznego dostawcę
Część podmiotów może zdecydować się na korzystanie z systemu wideokonferencji dostarczanego i obsługiwanego przez zewnętrznego dostawcę. W takim przypadku organ zaleca zawarcie umowy powierzenia przetwarzania danych z dostawcą usługi wideokonferencji (art. 28 ust. 3 RODO).

3. Usługa online
Niektóre podmioty zamiast samodzielnie obsługiwać system wideokonferencyjny lub zlecać jego obsługę zgodnie z własnymi pomysłami zewnętrznemu dostawcy usług, mogą korzystać z istniejących usług dostępnych online.

DSK zauważa, że wybór jednego ze wskazanych rozwiązań niesie ze sobą określone konsekwencje z punktu widzenia ochrony danych osobowych. Na przykład decydując się na pierwszy model, podmiot samodzielnie obsługuje system służący do wideokonferencji i z tego względu nie musi zawierać z innymi podmiotami ani umowy powierzenia, ani porozumienia o współadministrowaniu. Wybierając trzeci model, administrator danych musi natomiast rozważyć problem ewentualnego transferu danych osobowych do państw trzecich, jeżeli dostawca danej usługi wideokonferencji ma siedzibę w państwie trzecim.

[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).



Zgoda jako podstawa przetwarzania danych osobowych osób biorących udział w wideokonferencji

DSK zauważa, że jedną z potencjalnych podstaw przetwarzania danych osobowych osób biorących udział w wideokonferencji może być **zgoda** (art. 6 ust.1 lit. a RODO). Niemniej autorzy wytycznych zwracają uwagę na to, że w relacjach pracownik – pracodawca lub uczeń – szkoła zapewnienie dobrowolności zgody może być trudne, w szczególności gdy informacje niezbędne do wykonywania działalności zawodowej lub do udziału w lekcjach w szkole są przekazywane wyłącznie w drodze wideokonferencji.

Zdaniem DSK rozwiązaniem zapewniającym dobrowolność zgody podmiotu danych w takich przypadkach może być zapewnienie osobom, które nie chcą lub nie mogą uczestniczyć w wideokonferencji, dostępu do informacji, które zostały przekazane podczas spotkania, za pomocą innych kanałów komunikacji lub zaoferowanie tym osobom innych narzędzi (np. udział w spotkaniu przez połączenie telefoniczne). Jeżeli dobrowolny charakter korzystania z wideokonferencji nie może być zapewniony przez takie środki, korzystanie z wideokonferencji nie może być oparte na zgodzie jako podstawie prawnej.

Spełnienie obowiązku informacyjnego wobec uczestników wideokonferencji

DSK przypomina, że podmiot organizujący wideokonferencję musi spełnić w stosunku do osób w niej uczestniczących obowiązek informacyjny – odpowiednio z art. 13 lub 14 RODO – w sposób jednoznaczny i przejrzysty. DSK zwraca uwagę, że w klauzuli informacyjnej poza treściami wymaganymi przez wskazane przepisy powinny się znaleźć również następujące dodatkowe informacje:

- czy podczas wideokonferencji jest stosowane szyfrowanie, a jeśli tak, to jakiego rodzaju – DSK zauważa, że informacja ta ma szczególne znaczenie dla osób uczestniczących w wideokonferencji na podstawie zgody;
- o sposobach ochrony danych osobowych w ramach ustawień prywatności systemu wideokonferencji (np. poprzez użycie pseudonimu, ustawienie wirtualnego tła, jeżeli taka możliwość jest oferowana przez system wideokonferencji);
- czy konferencja może być nagrywana przez organizatora i w jaki sposób uczestnicy zostaną poinformowani o rozpoczęciu nagrywania.

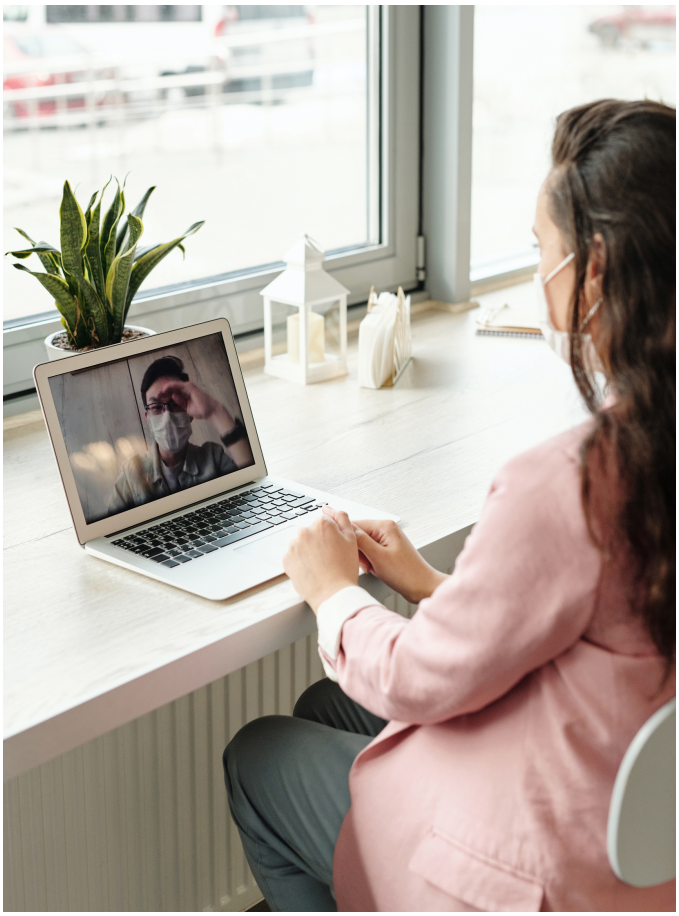
Uczestnictwo pracowników w wideokonferencji podczas home office

DSK zauważa, że w przypadku udziału w wideokonferencji pracownika oddelegowanego do pracy zdalnej inni uczestnicy takiego spotkania mają możliwość wglądu w jego życie osobiste.

Wobec tego pracodawcy jako administratorzy danych powinni informować swoich pracowników i innych uczestników, którzy mogą brać udział w wideokonferencji z własnych domów czy mieszkań, o potencjalnym ryzyku dla prywatności tych osób. Pracodawcy powinni zarekomendować pracownikom m.in.:

- zadbanie o odpowiednie ustawienie kamery;
- nieprzenoszenie sprzętu, którego pracownik używa do uczestnictwa w wideokonferencji, do pomieszczeń zajmowanych przez osoby trzecie.

Pełna wersja wytycznych DSK jest dostępna na stronie (wyłącznie w języku niemieckim): https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf



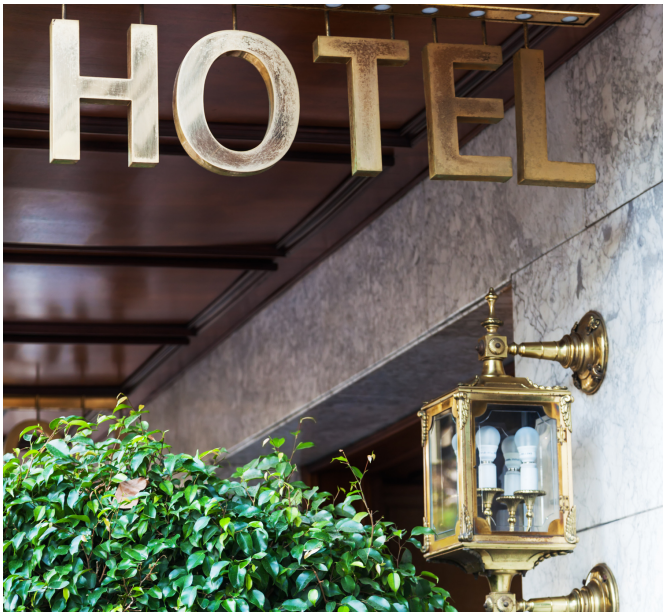
ICO nałożył na Marriott ponad 18 mln funtów kary za niezapewnienie odpowiednich zabezpieczeń danych osobowych klientów

dr Iga Małobęcka-Szwast, Senior Associate

W dniu 30 października 2020 r. brytyjski organ nadzorczy (ICO) nałożył na Marriott International, Inc. administracyjną karę pieniężną w wysokości 18,4 mln funtów za niezapewnienie odpowiednich zabezpieczeń danych osobowych klientów, tj. naruszenie art. 5 ust. 1 lit. f i art. 32 RODO[1]. Jest to jak dotąd druga najwyższa administracyjna kara pieniężna nałożona przez ICO pod rządami RODO.

Na czym polegało naruszenie?

Naruszenie bezpieczeństwa sięga 2014 r., kiedy to systemy Starwood Hotels and Resorts Worldwide, Inc. (sieć przejęta przez Marriott w 2016 r.) stały się celem cyberataku. Nieznany haker zainstalował fragment kodu na urządzeniu w systemie Starwood i poprzez złośliwe oprogramowanie uzyskał zdalny dostęp jako uprzywilejowany użytkownik systemu. Cyberprzestępca zdobył w ten sposób nie-ograniczony dostęp do poszczególnych urządzeń w sieci Starwood. Następnie zebrano dane logowania, a haker włamał się do bazy danych, w której przechowywane były dane rezerwacji, po czym ją wyeksportował.



Dane osobowe, których dotyczyło naruszenie, obejmowały: imiona i nazwiska, adresy e-mail, numery telefonów, niezaszyfrowane numery paszportów, informacje dotyczące przyjazdu i wyjazdu, status VIP gości i numer członkowski programu lojalnościowego.

Marriott szacuje, że cyberatakiem na Starwood Hotels and Resorts Worldwide, Inc. w 2014 r. zostało dotkniętych 339 mln rekordów gości na całym świecie, z czego 7 mln rekordów dotyczyło gości z Wielkiej Brytanii. Dokładna liczba osób dotkniętych naruszeniem jest trudna do ustalenia, ponieważ na jednego gościa mogło przypadać wiele rekordów.

Atak z nieznanego źródła został wykryty dopiero we wrześniu 2018 r., a Marriott powiadomił ICO i osoby, których dotyczyło naruszenie, w listopadzie 2018 r.

Dochodzenie ICO wykazało, że Marriott nie wdrożył odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przetwarzanych w jego systemach, zgodnie z wymogami art. 5 ust. 1 lit. f i art. 32 RODO.

W ocenie ICO naruszenie polegało m.in. na:

- niewystarczającym monitorowaniu kont użytkowników z uprzywilejowanym dostępem;
- niewystarczającym monitorowaniu baz danych;
- braku wdrożenia hartowania serwera jako środka zapobiegawczego (tj. zmniejszenie podatności serwera na ataki);
- braku szyfrowania niektórych danych osobowych, w tym niektórych numerów paszportów.

Z racji tego, że naruszenie miało miejsce przed opuszczeniem UE przez Wielką Brytanię, ICO przeprowadził postępowanie w imieniu wszystkich organów UE jako wiodący organ nadzorczy, zgodnie z art. 56 RODO. Kara i działania podjęte przez ICO zostały zatwierdzone przez inne unijne organy nadzorcze w ramach procesu współpracy z art. 60 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).

Wysokość kary

Kara pieniężna w wysokości 18,4 mln funtów jest jak dotąd drugą najwyższą karą nałożoną przez ICO pod rządami RODO[2]. Jest ona jednak znacznie mniejsza niż przewidywano. W lipcu 2019 r. ICO poinformował o zamiarze nałożenia kary pieniężnej w wysokości ponad 99 mln funtów.

Przy obliczaniu wysokości kary pieniężnej ICO zastosował pięciostopniowy proces określony w Polityce działań regulacyjnych (Regulatory Action Policy). ICO uwzględnił następujące czynniki:

- Marriott nie odniósł żadnych korzyści finansowych z naruszenia;
- istnieje wiele środków, które Marriott mógł zastosować, aby wykryć atak na wcześniejszym etapie;
- naruszenie dotyczyło bardzo dużej liczby osób;
- naruszenie wywołało stres po stronie osób, których dotyczyło naruszenie, czego dowodem było prawdopodobne zablokowanie kart płatniczych oraz 57 tys. połączeń odebranych przez centrum telefoniczne Marriott w następstwie naruszenia.

W ocenie ICO Marriott, nie zapewniając odpowiednich zabezpieczeń systemów, dopuścił się poważnego zaniedbania, w szczególności mając na względzie rozmiar i profil spółki oraz prawdopodobieństwo, że stanie się ona celem ataku.

Jakie czynniki łagodzące wziął pod uwagę ICO?

ICO zdecydował się na zmniejszenie proponowanej pierwotnie kary m.in. ze względu na:

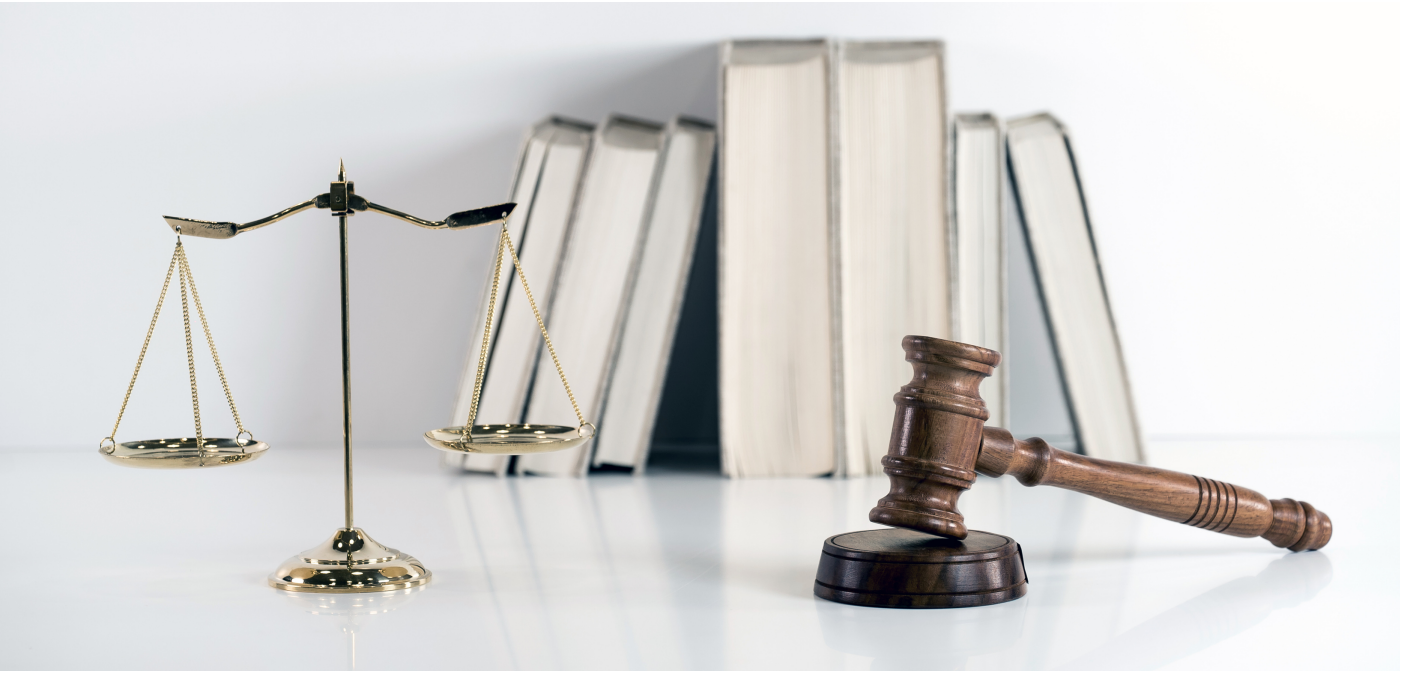
- kroki podjęte przez Marriott w celu złagodzenia skutków naruszenia;
- skutki ekonomiczne, jakie poniósł Marriott w wyniku pandemii COVID-19;
- fakt, że Marriott w pełni współpracował w ramach postępowania.

Działania podjęte przez Marriott w celu złagodzenia skutków naruszenia obejmowały:

- niezwłoczne skontaktowanie się z klientami po wykryciu naruszenia w celu zmniejszenia negatywnych skutków, które mogły dla tych osób wyniknąć wskutek tego zdarzenia;
- zresetowanie haseł i wyłączenie zagrożonych kont;
- wdrożenie ulepszonych narzędzi do wykrywania naruszeń;
- utworzenie specjalnej witryny internetowej oraz call center służących do zgłaszania naruszeń w różnych językach.

Źródło:
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/

[2] Najwyższą karą nałożoną przez ICO jest jak dotąd kara nałożona na British Airways, o której pisaliśmy w poprzednim numerze newslettera RODO.



Automatycznie zaznaczony checkbox a zgoda na przetwarzanie danych osobowych – wnioski po wyroku TSUE z dnia 11 listopada 2020 r. w sprawie Orange România SA (sygn. C-61/19)

apl. radc. Michał Matysiak, Associate

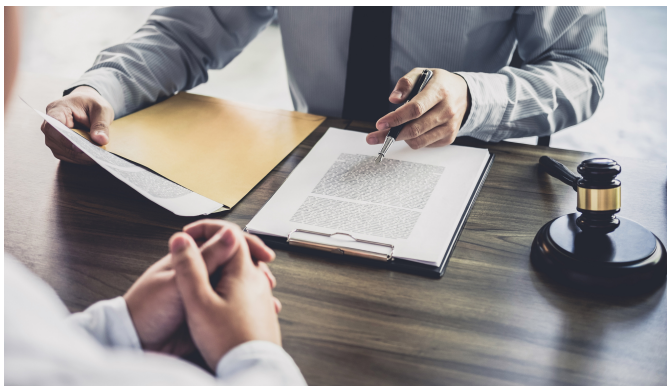
Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w wyroku z dnia 11 listopada 2020 r. w sprawie Orange România SA przeciwko rumuńskiemu organowi ochrony danych (C-61/19) potwierdził, że automatycznie zaznaczone okienko (checkbox) nie może zostać uznane za jednoznaczne wyrażenie zgody w rozumieniu art. 4 pkt 11 RODO.

Wprowadzenie

Orange România SA jest operatorem telefonii komórkowej na rynku rumuńskim. W dniu 28 marca 2018 r. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Krajowy Urząd ds. Nadzoru nad Przetwarzaniem Danych Osobowych, dalej: „ANSPDCP") nałożył na operatora grzywnę za gromadzenie i przechowywanie kopii dokumentów tożsamości swoich klientów bez ich wyraźnej zgody.

W ocenie ANSPDCP w okresie od 1 do 26 marca 2018 r. Orange România SA zawierała umowy o świadczenie usług telefonii komórkowej, które zawierały klauzulę stanowiącą, że klienci zostali poinformowani o sporządzeniu i przechowywaniu kopii ich dokumentów tożsamości w celu identyfikacji oraz wyrazili zgodę na ich przetwarzanie. Pole (checkbox) odnoszące się do tej klauzuli zostało zaznaczone przez administratora danych przed podpisaniem umowy.

To właśnie w tym kontekście Sąd Okręgowy w Bukareszcie (Tribunalul București) zwrócił się do TSUE z wnioskiem o określenie warunków, w których zgoda klientów na przetwarzanie danych osobowych może zostać uznana za ważną.



Wyrok w sprawie Orange România SA

W wyroku Trybunał stwierdził, że prawo Unii (rozumiane jako RODO) przewiduje wykaz przypadków, w których przetwarzanie danych osobowych może być uznane za zgodne z prawem. W szczególności zgoda osoby, której dane dotyczą, musi być **dobrowolna, konkretna, świadoma i jednoznaczna**. Ponadto, jeżeli zgoda osoby, której dane dotyczą, jest udzielana w kontekście pisemnego oświadczenia obejmującego również inne kwestie, **oświadczenie to musi być przedstawione w zrozumiałej i łatwo dostępnej formie, przy użyciu jasnego i prostego języka.**

Trybunał podkreślił, że ponieważ Orange România SA jest administratorem danych osobowych, musi być w stanie wykazać zgodność z prawem przetwarzania tych danych, a zatem, w niniejszej sprawie, istnienie ważnej zgody swoich klientów. W tym względzie Trybunał uznał, że nie wydaje się, by zainteresowani klienci operatora sami zaznaczyli pole dotyczące gromadzenia i przechowywania danych w zakresie kopii dokumentów tożsamości tych osób. **Sama okoliczność, że formularz zawiera zaznaczone pole, nie może stanowić pozytywnej wskazówki co do ich aktywnej zgody.**

W ocenie Trybunału do sądu krajowego powinna należeć ocena, czy sporne postanowienia umowne mogły wprowadzić w błąd zainteresowanych klientów co do możliwości zawarcia umowy, pomimo odmowy wyrażenia zgody na przetwarzanie ich danych, w braku konkretnych szczegółów dotyczących tej możliwości.

W przypadku odmowy wyrażenia zgody operator wymagał od klienta złożenia pisemnego oświadczenia, że nie wyraził on zgody na pobranie lub przechowywanie kopii swojego dokumentu tożsamości. Jak zauważył Trybunał, taki dodatkowy wymóg może nadmiernie ograniczyć swobodę wyboru w zakresie sprzeciwu wobec przedmiotowych czynności przetwarzania. Trybunał podkreślił, że skoro Orange România SA jako administrator jest **zobowiązany do wykazania aktywnej zgody klientów w zakresie przetwarzania ich danych osobowych, to nie mógł wymagać od tych osób aktywnego wyrażenia odmowy.**

[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); Dz.Urz.UE.L Nr 119, str. 1; dalej: „RODO".

W motywie 56 wyroku Trybunał wskazał przypadki, gdy **umowa o świadczenie usług telekomunikacyjnych** zawierająca klauzulę stwierdzającą, że osoba, której dane dotyczą, została poinformowana o skopiowaniu i przechowywaniu kopii swego dokumentu tożsamości do celów identyfikacji i wyraziła na to zgodę, **nie pozwala wykazać, że osoba ta skutecznie wyraziła zgodę,** w rozumieniu wskazanych przepisów, na sporządzenie tej kopii i jej przechowywanie. Są to sytuacje, gdy:

- okienko wyboru odnoszące się do tej klauzuli zostało zaznaczone przez administratora danych przed podpisaniem umowy;
- postanowienia rzeczonej umowy mogą wprowadzać osobę, której dane dotyczą, w błąd co do możliwości zawarcia owej umowy pomimo odmowy udzielenia zgody na przetwarzanie danych;
- administrator bezpodstawnie wpłynął na swobodne podjęcie decyzji o sprzeciwieniu się skopiowaniu i przechowywaniu kopii dokumentu tożsamości poprzez ustanowienie wymogu, aby w wypadku odmowy udzielenia zgody osoba, której dane dotyczą, wypełniła dodatkowy formularz dokumentujący tę odmowę.

Wnioski

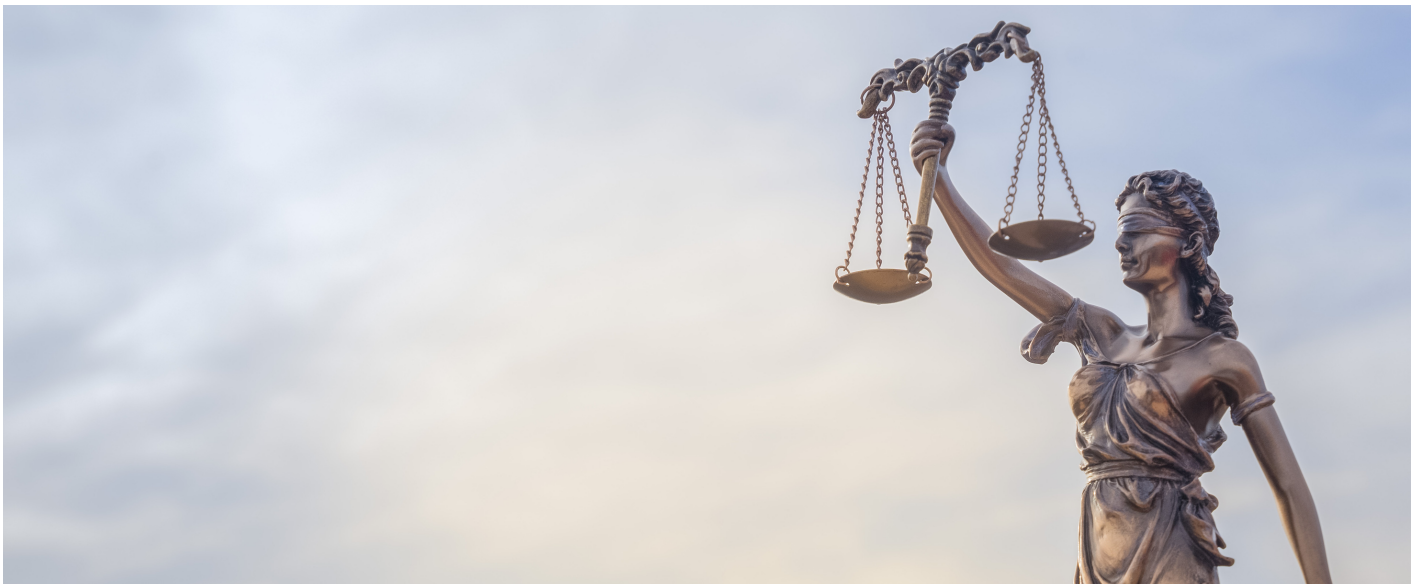
Przedmiotowe orzeczenie trudno uznać za rewolucję, a bardziej za potwierdzenie pewnego dosyć dobrze ugruntowanego podejścia do kwestii pozyskiwania zgód z wykozystaniem okienek do zaznaczania (checkbox).

Przedmiotowe orzeczenie dotyka bardzo istotnej kwestii formy, w jakiej może zostać wyrażona zgoda na przetwarzanie danych osobowych. Trybunał przypomina, że zgodnie z definicją zawartą w art. 4 pkt 11 RODO zgoda to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli. O ile powyższy przepis nie wyjaśnia jednoznacznie, w jakiej formie powinna zostać wyrażona zgoda, o tyle dosyć dobitnie akcentuje to motyw 32 RODO, który odwołuje się do „jednoznacznej, **potwierdzającej** czynności" oraz w dalszej części przesądza, że „milczenie, **okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny oznaczać zgody".**

W kontekście omawianego wyroku szczególnie istotne są dwa elementy zgody, tj. jej jednoznaczność oraz forma wyrażenia. „Jednoznaczność jako cecha okazania woli oznacza, że nie może ono pozostawiać wątpliwości co do zamiaru wyrażenia zgody przez osobę, której dane dotyczą"[2] . W doktrynie wskazuje się, że automatycznie zaznaczone okienka nie mogą zostać uznane za działanie wyraźnie potwierdzające wyrażenie zgody w rozumieniu art. 4 pkt 11 RODO przez podmioty przetwarzania danych .

Takie stanowisko powtarza również wyrok w sprawie Orange România SA, który ponadto kwestionuje praktykę wypełniania dodatkowego formularza dokumentującego odmowę udzielenia zgody. Wymóg ten może bowiem nadmiernie ograniczyć swobodę wyboru w zakresie sprzeciwu wobec czynności przetwarzania oraz jest sprzeczny z istotą ciążącego na administratorze obowiązku wykazania aktywnej zgody klienta.

[2] B. Fischer, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda, Komentarz do art. 4 [w:] M. Sakowska-Baryła (red.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Warszawa 2018, Legalis.



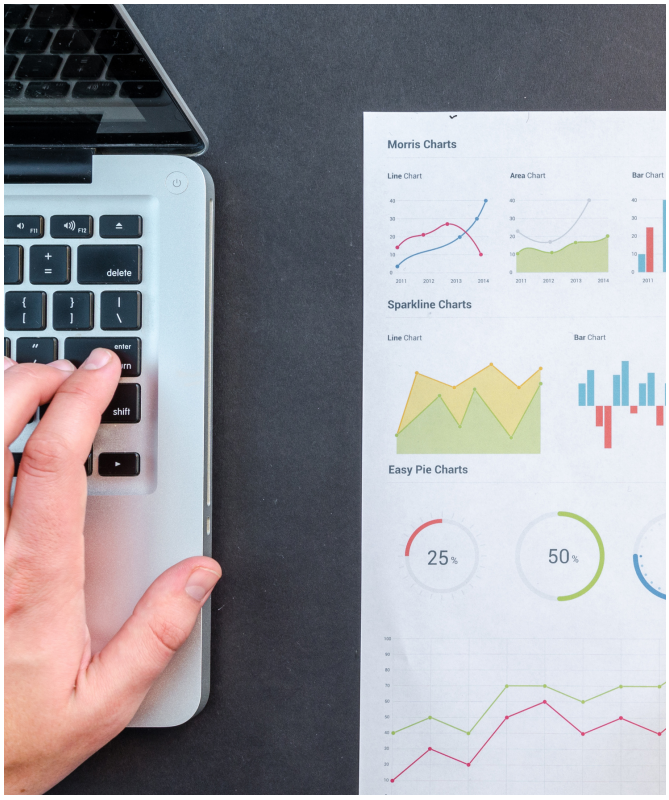
Raport BSI na temat bezpieczeństwa IT w Niemczech w 2020 r.

Mateusz Kupiec, Trainee

Federalny Urząd Bezpieczeństwa Teleinformatycznego (Bundesamt für Sicherheit in der Informationstechnik, dalej: „BSI") opublikował raport dotyczący poziomu bezpieczeństwa sektora IT w Niemczech. Stan cyberbezpieczeństwa w tym państwie ma znaczenie dla polskich przedsiębiorstw, które współpracują z podmiotami z Niemiec. Przedstawiamy wybrane ustalenia organu.

Podsumowanie stanu bezpieczeństwa IT i ocena sytuacji w zakresie ryzyka

Zdaniem BSI w okresie powstawania raportu, tj. od 1 czerwca 2019 r. do 31 maja 2020 r., sytuacja w zakresie bezpieczeństwa IT w Niemczech pozostawała napięta. Zagrożenie wyciekiem danych osiągnęło nowy poziom, atakujący coraz częściej wykorzystywali także „czynnik ludzki" jako furtkę do przeprowadzenia skutecznego cyberataku przy wykorzystaniu różnych socjotechnik. Z ustaleń BSI wynika m.in., że:



1. Ataki typu DDoS (distributed denial of service) stają się coraz bardziej wysublimowane.

W szczególności zaobserwowano, że atakujący wykorzystywali publicznie dostępne informacje, takie jak raporty z incydentów, w celu analizy środków bezpieczeństwa ofiary oraz do elastycznego dostosowywania swoich strategii ataku na zasadzie ad hoc. Ataki typu DDoS polegają na wysyłaniu z wielu miejsc w Internecie jednocześnie bardzo dużej liczby zapytań do atakowanego serwera, co prowadzi do jego niedostępności lub niestabilności.

2. Wzrosła liczba wycieków danych

Wśród przedsiębiorstw dotkniętych wyciekiem danych znalazły się: znane banki, dostawcy usług płatniczych, firmy technologiczne, gabinety lekarskie, szpitale, uniwersytety, a także podmioty z sektora e-commerce.

3. Cyberprzestępcy coraz częściej korzystają z metod szyfrowania

W 2020 r. wśród cyberprzestępców wzrosła tendencja do korzystania ze stron szyfrowanych za pomocą protokołu HTTPS (internetowy protokół komunikacyjny mający na celu ochronę poufności i integralności danych przesyłanych między urządzeniem a konkretną witryną internetową). Z ustaleń organu wynika, że ponad co drugi link w wiadomościach e-mail wysyłanych w celu przeprowadzenia ataku typu phishing prowadzi obecnie do wzbudzającej zaufanie, zabezpieczonej protokołem HTTPS strony internetowej, która w rzeczywistości służy wyłudzeniu danych.

Wyniki projektu BSI dotyczącego sposobu ochrony kont online

BSI wspólnie z Urzędem Kanclerza Federalnego (Bundeskanzleramt) zrealizował projekt mający na celu pozyskanie informacji dotyczących m.in. obsługi haseł, percepcji ryzyk związanych z cyberbezpieczeństwem przez obywateli. W ramach projektu przeprowadzono z łącznie 100 osobami ro-zmowy, na podstawie których ustalono, że:

- 67% respondentów twierdzi, że używa haseł, które całkowicie różnią się od siebie;

- 10% uczestników badania tworzy hasła według własnych zasad;
- spośród 39% ankietowanych, którzy wiedzą o istnieniu menedżerów haseł, korzysta z nich tylko 27%;
- 74% respondentów zapamiętuje swoje hasła, 34% – zapisuje hasła na papierze, 15% – przechowuje je w menedżerze haseł (możliwe było udzielanie wielokrotnych odpowiedzi);
- 78% ankietowanych obawia się, że haker może zdobyć wszystkie hasła użytkownika w wyniku skutecznego ataku na program służący do zarządzania hasłami.

Cyberbezpieczeństwo w liczbach

Zgodnie z szacunkami BSI w Niemczech w okresie prac nad raportem:

- powstało ok. 117,4 miliona nowych rodzajów szkodliwego oprogramowania;
- średnio 35 tysięcy e-maili ze złośliwym oprogramowaniem było miesięcznie wyłapywanych przez niemieckie sieci rządowe;
- odsetek niechcianych wiadomości wśród wszystkich trafiających do sieci rządu federalnego wynosi 76%.

Komentarz

Administratorzy danych osobowych powinni starać się mieć aktualną wiedzę o stanie cyberbezpieczeństwa w państwach, w których świadczą usługi, oferują towary lub z których pochodzą współpracujące z nimi podmioty. Informacje w tym zakresie mogą bowiem pomóc administratorom w lepszej ocenie ryzyka dla bezpieczeństwa przetwarzanych przez nich danych osobowych.

Pełna wersja raportu BSI jest dostępna na stronie (wyłącznie w języku niemieckim):
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2.

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

Michał Matysiak
Aplikant Radcowski, Associate
michał.matysiak@traple.pl

Mateusz Kupiec
Trainee
mateusz.kupiec@traple.pl

Redaktor newslettera:
dr Iga Małobęcka-Szwast

Pytania prosimy kierować na adres:
rodo@traple.pl