Godziny urzędowania	Informacja w Sprawach Pn.- Pt. 8^{00}-16^{00}	Czytelnia Akt Pn.- Pt. 8^{00} - 15^{30}	Biuro Podawcze
Telefon			
Email	.pl	pl	

Wynik rozprawy dostępny po zakończeniu posiedzenia Sądu, najpóźniej w dniu następnym na stronie:

Wojewódzki Sąd Administracyjny
w Warszawie
WYDZIAŁ II
ul. Jasna 2/4
00-013 Warszawa

Dnia

Sygn. akt **II SA/Wa 3993/21**

W odpowiedzi należy podać
sygnaturę akt sądu

DORĘCZENIE ODPISU WYROKU

W wykonaniu zarządzenia sekretariat Wydziału II Wojewódzkiego Sądu Administracyjnego doręcza Panu – jako Pełnomocnikowi skarżącego – odpis wyroku z dnia 11 lipca 2022 r. wraz z uzasadnieniem.

starszy specjalista

ODPIS

Sygn. akt II SA/Wa 3993/21

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 11 lipca 2022 r.

Wojewódzki Sąd Administracyjny w Warszawie
w składzie następującym:

Przewodniczący Sędzia WSA
Sędzia WSA
Asesor WSA i (spr.)

Protokolant referent stażysta

po rozpoznaniu na rozprawie w dniu 5 lipca 2022 r.
sprawy ze skargi iSecure sp. z o.o. z siedzibą w Warszawie
na decyzję Prezesa Urzędu Ochrony Danych Osobowych
z dnia 29 września 2021 r. nr DS.523.3908.2021.PR.KM.141473
w przedmiocie przetwarzania danych osobowych

1. **uchyla zaskarżoną decyzję;**
2. **zasądza od Prezesa Urzędu Ochrony Danych Osobowych na rzecz skarżącej iSecure sp. z o.o. z siedzibą w Warszawie kwotę 697 zł (słownie: sześćset dziewięćdziesięciu siedmiu złotych) tytułem zwrotu kosztów postępowania sądowego.**

Na oryginale właściwe podpisy
Za zgodność z oryginałem
starszy specjalista

WOJEWÓDZKI SĄD ADMINISTRACYJNY W WARSZAWIE * 2 *

Sygn. akt II SA/Wa 3993/21

UZASADNIENIE

(dalej również „uczestnik postępowania") w piśmie z 28 czerwca 2021 r. wniósł do Prezesa Urzędu Ochrony Danych Osobowych (dalej „PUODO") skargę na nieprawidłowości w procesie przetwarzania jego danych osobowych przez iSecure sp. z o.o. z siedzibą w Warszawie (dalej również „Spółka" lub „iSecure") - administratora strony internetowej znajdującej się pod adresem: https://www.isecure.pl - polegające na udostępnieniu danych osobowych podmiotom trzecim bez podstawy prawnej poprzez ich ujawnienie przez stronę internetową znajdującą się pod adresem https://www.isecure.pl/blog/jak-stworzyc-strone-internetowa-zgodna-z-rodo-czesc-i-regulaminy, niespełnieniu żądania w zakresie prawa dostępu do danych wynikającego z art. 15 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „RODO"), w tym na nieudostępnieniu kopii jego danych osobowych, które przetwarzane są przez Spółkę i udostępnione zostały podmiotom trzecim, a także niespełnieniu żądania usunięcia jego danych osobowych z bazy danych Spółki.

oświadczył, że 22 maja 2021 r. Spółka udostępniła poprzez wyżej wymienioną stronę internetową jego dane osobowe następującym podmiotom:

1. właścicielowi domeny w zakresie jego adresu IP oraz części historii przeglądania opatrzonej sztucznie nadanym ID z cookies,
2. właścicielowi domeny w zakresie jego adresu IP oraz części historii przeglądania opatrzonej sztucznie nadanym ID z cookies,
3. właścicielowi domeny w zakresie jego adresu IP oraz części historii przeglądania,
4. właścicielowi domeny w zakresie jego adresu IP oraz części historii przeglądania,
5. właścicielowi domeny w zakresie jego adresu IP oraz części historii przeglądania,
6. właścicielowi domeny w zakresie jego adresu IP oraz części historii przeglądania,
7. właścicielowi domeny , w zakresie jego adresu IP oraz części historii przeglądania.

Na dowód powyższego uczestnik postępowania dołączył do skargi tzw. zrzuty ekranu zawierające widok strony internetowej z uruchomionym narzędziem

analitycznym przeglądarki internetowej. Podał, że wyżej wymienione dane zostały przesłane natychmiast (zanim miał szansę przeczytać politykę prywatności), bez jego zgody i w jego ocenie bez ważnej przesłanki legalizującej. Wskazał, że podmioty oraz nie są wymienione w polityce prywatności dostępnej na stronie internetowej iSecure. Dodał, że wysłał do iSecure wiadomość elektroniczną, w której zażądał udzielenia informacji, jakie przesłanki legalizujące zostały użyte do przetwarzania jego danych osobowych, usunięcia jego danych osobowych przekazanych przez stronę iSecure do podmiotów trzecich oraz wskazania tożsamości podmiotów, do których jego dane zostały wysłane. Skonstatował, że jakkolwiek Spółka odpowiedziała na wiadomość, to jego żądania nie zostały spełnione.

dołączył do skargi opisaną poniżej korespondencję elektroniczną prowadzoną z iSecure.

W skierowanej do Spółki wiadomości e-mail z 22 maja 2021 r. uczestnik postępowania stwierdził, że wyżej wymienione informacje są automatycznie wysyłane przez skrypty umieszczone na stronie internetowej iSecure i pomimo, że Spółka nie otrzymuje ich bezpośrednio i nie przechowuje tych danych, w świetle RODO jest ich administratorem. W jego ocenie, brak jest przesłanki legalizującej przetwarzanie wyżej wymienionych danych osobowych. zażądał prawa dostępu do danych w zakresie wskazania odbiorców, którym udostępnione zostały jego dane i przesłanek uzasadniających to udostępnienie, jeśli takie istnieją, jak również udostępnienia kopii jego danych osobowych, które przetwarzane są przez Spółkę i udostępnione zostały podmiotom trzecim. Jednocześnie wniósł o usunięcie przesłanych danych z bazy wyżej wymiennych podmiotów, którym zostały one udostępnione.

W wiadomości z 28 czerwca 2021 r. uczestnik postępowania zarzucił także, że Spółka nie zamieściła w swojej polityce prywatności informacji o korzystaniu przez stronę internetową z cookies, aby przesłać opatrzone unikalnym identyfikatorem dane do i

W skierowanej do wiadomości z 21 czerwca 2021 r. Spółka stwierdziła, że do czasu przysłania wiadomości z 22 maja 2021 r. nie przetwarzała żadnych jego danych osobowych. Poinformowała, że informacje przetwarzane o użytkownikach strony internetowej nie pozwalają jej na identyfikację konkretnej osoby fizycznej, a innymi słowy osoba taka nie jest dla niej identyfikowalna. Dlatego informacje te nie stanowią danych osobowych. iSecure wskazała, że zgodnie z tym, o czym informuje użytkownika natychmiastowo przy pierwszym wejściu na stronę, strona www.isecure.pl stosuje pliki cookies, a Spółka bazuje na zgodzie użytkownika na

wykorzystywanie plików cookies, wyrażonej za pomocą ustawień własnej przeglądarki użytkownika.

PUODO w piśmie z 7 lipca 2021 r., działając na podstawie art. 58 ust. 1 lit. a i lit. e RODO zwrócił się do iSecure o ustosunkowanie się do skargi oraz złożenie wyjaśnień. W związku z brakiem formalnym (niewłaściwe podpisanie) odpowiedzi udzielonej w piśmie z 29 lipca 2021 r. wezwanie zostało ponowione w piśmie PUODO z 3 sierpnia 2021 r. Organ nadzorczy zażądał udzielenia informacji:

1. czy, a jeśli tak, to kiedy, na jakiej podstawie prawnej, z jakiego źródła, w jakim celu i zakresie Spółka pozyskała dane osobowe , w tym dane w zakresie jego adresu IP, historii przeglądania stron internetowych oraz sztucznie nadanego ID z cookies;
2. czy Spółka aktualnie przetwarza dane osobowe , w tym dane w zakresie jego adresu IP, historii przeglądania stron internetowych oraz sztucznie nadanego ID z cookies, a jeśli tak, to na jakiej podstawie prawnej, w jakich celach oraz jak długo te dane będą przetwarzane;
3. czy, a jeśli tak, to kiedy, na jakiej podstawie prawnej, w jakim celu i zakresie oraz jakim podmiotom Spółka udostępniła przez stronę internetową znajdującą się pod adresem: https://www.isecure.pl/blog/jak-stworzyc-strone-intemetowa-zgodna-z-rodo-czesc-I-regulaminy dane osobowe , w tym w zakresie jego adresu IP, historii przeglądania stron internetowych oraz sztucznie nadanego ID z cookies;
4. czy, kiedy oraz w jaki sposób Spółka odniosła się do żądania z 22 maja 2021 r. w zakresie prawa dostępu do danych wynikającego z art. 15 ust. 1 RODO dotyczącego wskazania odbiorców, którym jego dane zostały udostępnione oraz przesłanek legalizujących to udostępnienie, jak również udostępnienia kopii jego danych osobowych, które przetwarzane są przez Spółkę i udostępnione zostały podmiotom trzecim;
5. czy, kiedy oraz w jaki sposób Spółka odniosła się do żądania z 22 maja 2021 r. w zakresie usunięcia jego danych osobowych z bazy danych Spółki i podmiotów, którym zostały one udostępnione;
6. czy, a jeśli tak, to kiedy oraz w jaki sposób Spółka poinformowała podmioty, którym udostępniła dane osobowe (o ile je udostępniła) o jego żądaniu w zakresie usunięcia tych danych.

Ponadto PUODO wezwał iSecure do złożenia:

1. poświadczonej za zgodność z oryginałem kopii umowy powierzenia przetwarzania danych zawartego pomiędzy Spółką a właścicielem domeny

2. poświadczonej za zgodność z oryginałem kopii dokumentacji, na podstawie której dochodzi do wymiany danych osobowych w zakresie jego adresu IP, historii przeglądania stron internetowych oraz sztucznie nadanego ID z cookies, pomiędzy Spółką a właścicielami innych wyżej wymienionych domen internetowych.

W odpowiedzi udzielonej w pismach z 13 sierpnia 2021 r. Spółka oświadczyła, że przetwarzany przez nią adres IP oraz sztucznie nadany cookies ID nie stanowią - w jej ocenie - danych osobowych uczestnika postępowania. Stwierdziła, że nie pozyskała historii przeglądania stron internetowych ., ponieważ nie ma takiej możliwości. Wskazała, że jedyną pozyskaną informacją o użytkowniku było IP/ID użytkownika, który jednak nie daje Spółce możliwości zweryfikować (zidentyfikować) odwiedzającego stronę, a w związku z tym nie może być tu mowy o przetwarzaniu danych osobowych uczestnika postępowania. Zauważyła, że numer IP/ID nie stanowi dla niej danych osobowych, ponieważ ani Spółka, ani wskazane w skardze podmioty (tj. właściciel domeny właściciel domeny , właściciel domeny google-analytics.com, właściciel domeny właściciel domeny właściciel domeny , właściciel domeny) nie mają możliwości zidentyfikowania końcowego użytkownika. Zaznaczyła, że należy mieć w tym względzie na uwadze m.in. zmienność adresu IP oraz numeru ID, czy liczbę osób korzystających z komputera/przeglądarki internetowej. Spółka podkreśliła, że udostępniła jedynie informacje, lecz nie dane osobowe, w postaci cookie ID. Wskazała, że właściciel domeny , o której pisze , to dostawca oprogramowania dla iSecure, służącego do przesyłania wiadomości on-line podczas wizyty na stronie lub zamówienia rozmowy telefonicznej. Jak wyjaśniła Spółka, w przypadku, gdy nie zostanie rozpoczęty czat, to żadne informacje poza adresem IP odwiedzającego stronę nie są przekazywane temu dostawcy. Tym bardziej w takiej sytuacji nie są przekazywane dane osobowe. Podała, że wszystkie inne domeny wymienione przez wynikają z wykorzystywania plików cookies analitycznych na stronie Spółki. Zaznaczyła, że wysyłane jest jedynie zapytanie dotyczące cookie ID, a nie jak twierdzi uczestnik postępowania historia przeglądania stron www, co zostało potwierdzone przez firmę obsługującą stronę internetową iSecure.

Spółka wywiodła również, że odniosła się do żądania poprzez wyjaśnienie, iż nie przetwarzała danych osobowych będących przedmiotem jego żądania, czyli adresu IP, część historii przeglądania, sztucznie nadanego ID z cookies, a zatem nie przekazała takich informacji, jako danych osobowych, innym podmiotom (informacje te nie stanowią danych osobowych, gdyż Spółka nie jest w stanie

zidentyfikować uczestnika postępowania po informacjach, które pozyskała za pomocą strony www). iSecure skonstatowała, że zgodnie z unikalnym identyfikatorem, który został przekazany za pomocą cookies analitycznego, nie można dokonać identyfikacji użytkownika końcowego, którym jest uczestnik postępowania.

Spółka wyjaśniła też, że pliki cookies są wykorzystywane zgodnie z ustawieniami przeglądarki na urządzeniu końcowym użytkownika. Każdy użytkownik odwiedzający stronę www Spółki ma możliwość świadomej konfiguracji swojej własnej przeglądarki, z której korzysta. Posiada widoczną dla użytkownika podczas wchodzenia przez niego na stronę www Spółki informację nie tylko o tym, że strona wykorzystuje pliki cookies, ale także pouczenie i przypomnienie użytkownikom o tym, że można zmienić samodzielnie ustawienia przeglądarki.

Spółka dołączyła do udzielonej odpowiedzi m.in. dokumenty mające świadczyć jej zdaniem o braku możliwości identyfikacji uczestnika postępowania na podstawie adresu IP oraz ID plików cookies.

Prezes Urzędu Ochrony Danych osobowych decyzją z 29 września 2021 r. nr DS.523.3908.2021.PR.KM.141473, na podstawie art. 104 § 1 K.p.a. w zw. z art. 7 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, art. 6 ust. 1, art. 15 ust. 1 lit. c, art. 15 ust. 3, art. 17 ust. 1, art. 19 oraz art. 58 ust. 2 lit. b i lit. c RODO:

1. nakazał iSecure usunięcie danych osobowych , w zakresie jego adresu IP oraz sztucznie nadanego ID z cookies;
2. nakazał iSecure poinformować podmioty, którym udostępniła dane osobowe , w zakresie jego adresu IP oraz sztucznie nadanego ID z cookies, o ich usunięciu;
3. udzielił iSecure upomnienia za naruszenie art. 15 ust. 1 lit. c RODO polegającego na niespełnieniu żądania w zakresie wskazania mu informacji dotyczących właściciela domeny oraz , którym udostępnione zostały jego dane osobowe;
4. udzielił iSecure upomnienia za naruszenie art. 6 ust. 1 RODO, polegającego na udostępnieniu podmiotom trzecim bez podstawy prawnej danych osobowych w zakresie adresu IP oraz sztucznie nadanego ID z cookies;
5. udzielił iSecure upomnienia za naruszenie art. 15 ust. 3 RODO, polegającego na niespełnieniu żądania , w zakresie udostępnienia kopii jego danych osobowych.

W uzasadnieniu decyzji organ nadzorczy opisał dotychczasowy przebieg postępowania, po czym stwierdził, że w pierwszej kolejności należało wyjaśnić, czym

jest adres IP. Przywoławszy następnie treść art. 4 pkt 1 oraz motywu 30 RODO, PUODO odwołał się do wyroku Naczelnego Sądu Administracyjnego z 19 maja 2011 r. sygn. akt I OSK 1079/10 wywodząc, że informacje, które wiążą się z określoną osobą - choćby pośrednio - niosą pewien komunikat o niej. Dlatego też informacją dotyczącą osoby jest zarówno informacja odnosząca się do niej wprost, jak i taka, która odnosi się bezpośrednio do przedmiotów czy urządzeń, ale poprzez możliwość powiązania tych przedmiotów czy urządzeń z określoną osobą pośrednio stanowi informację także o niej samej. Adres IP (Internet Protocol Address) jest unikatowym numerem przyporządkowanym urządzeniom sieci komputerowych. Jest zatem informacją dotyczącą komputera, a nie konkretnej osoby fizycznej, zwłaszcza wtedy gdy możliwe jest współużyczenie jednego adresu IP przez wielu użytkowników w ramach sieci lokalnej. Tam, gdzie adres IP jest na dłuższy okres lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową, jest to bowiem informacja umożliwiająca identyfikację konkretnej osoby fizycznej.

Jak skonstatował organ nadzorczy, w związku z powyższym, w jego ocenie stwierdzić należy, że zarówno adres IP uczestnika postępowania, jak również ID plików cookies, z uwagi na uzasadnione prawdopodobieństwo zidentyfikowania uczestnika postępowania w powiązaniu z tymi danymi, stanowią jego dane osobowe.

Następnie PUODO stwierdził, że dla dalszych rozważań istotne jest, że 1 października 2019 r. Trybunał Sprawiedliwości Unii Europejskiej (dalej Trybunał) wydał wyrok sprawie C-673/17 [redacted] w którym wskazał, że instalowanie plików cookie, o których mowa w postępowaniu głównym, wiąże się z przetwarzaniem danych osobowych.

Dalej, odwołując się do powołanego wyroku, a także do wytycznych nr 05/2020 przyjętych przez Europejską Radę do Spraw Ochrony Danych Osobowych 4 maja 2020 r., PUODO zaznaczył, że zgoda osoby, której dane dotyczą, może sprawić, że takie przetwarzanie danych stanie się zgodne z prawem, pod warunkiem że zgoda taka została jednoznacznie wyrażona przez ową osobę, której dane dotyczą. Wymóg ten może spełniać jedynie czynne zachowanie tej osoby podjęte w celu wyrażenia zgody. Organ nadzorczy stwierdził, że podziela stanowisko Trybunału, iż zgodna użytkownika witryny na instalowanie plików cookies na jego urządzeniu powinna być wyrażona w sposób czynny i jednoznaczny, a brak aktywnego działania ze strony użytkownika skutkować będzie jej nieważnością.

PUODO stwierdził również, że istotne znaczenie w sprawie ma art. 174 ustawy

z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (dalej „Prawo telekomunikacyjne"), zgodnie z którym do uzyskania zgody abonenta lub użytkownika końcowego stosuje się przepisy o ochronie danych osobowych. Jak skonstatował PUODO, regulacja ta oznacza, że zgoda musi spełniać kryteria wyznaczone przez art. 4 pkt 11 RODO, w świetle którego zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Następnie PUODO stwierdził, że zgodę udzieloną poprzez fakt, iż osoba odwiedzająca stronę internetową iSecure nie dokona zmiany ustawień swojej przeglądarki, a więc zaniecha podjęcia wskazanego przez Spółkę działania, uznać należy za zgodę wyrażoną w sposób bierny i milczący. Jak skonstatował organ nadzorczy, zgody wyrażonej we wskazany przez Spółkę sposób nie można zatem uznać za ważną w świetle obowiązujących przepisów RODO. Nie spełnia ona bowiem warunków wynikających z art. 4 pkt 11 RODO, tj. wymogu dobrowolności, świadomości, jednoznaczności oraz konkretności, ani - jak wskazał Trybunał w sprawie F - wymogu aktywnego i wyraźnego działania ze strony użytkownika, którego dane podlegać będą przetwarzaniu.

Dalej odwołując się do wyroku w sprawie PUODO wywiódł, że w odniesieniu do obowiązków informacyjnych wynikających z instalowania i udostępniania plików cookies na urządzeniach użytkowników witryny internetowej, Trybunał stwierdził, że jasne i wyczerpujące informacje powinny umożliwiać użytkownikowi łatwe ustalenie konsekwencji zgody, której może udzielić, oraz gwarantować, że zgoda ta zostanie udzielona przy pełnej znajomości stanu rzeczy. Informacje te muszą być wyraźnie zrozumiałe i wystarczająco dokładne, aby umożliwić użytkownikowi zrozumienie funkcjonowania plików cookie, które są wykorzystywane. Jeżeli chodzi o możliwość dostępu stron trzecich do plików cookie lub jej brak - jest to informacja należąca do informacji, o których mowa w art. 10 lit. c) dyrektywy 95/46 i w art. 13 ust. 1 lit. e) RODO, skoro przepisy te wyraźnie wymieniają odbiorców lub kategorie odbiorców danych.

Odwoławszy się następnie do art. 173 ust. 1 i ust. 2 Prawa telekomunikacyjnego oraz art. 5 ust. 3 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), PUODO stwierdził, że wobec powyższego

osoba, której dane podlegać będą przetwarzaniu musi zostać o tym fakcie poinformowana zanim nastąpi instalacja plików cookies na jej urządzeniu. Jak stwierdził organ nadzorczy, z zebranego w sprawie materiału dowodowego wynika natomiast, że dane zostały udostępnione wskazanym przez niego w skardze podmiotom zanim miał możliwość zapoznać się z polityką prywatności zamieszczoną na stronie internetowej Spółki. Ponadto - jak wskazał PUODO odwołując się do twierdzenia - w dostępnej na 22 maja 2021 r. polityce prywatności nie widniała informacja o udostępnieniu danych osobowych dwóm z wymienionych przez niego podmiotom, tj. oraz PUODO skonstatował, że uczestnik postępowania, przed instalacją plików cookies i udostępnieniem jego danych podmiotom trzecim, nie został więc uprzednio poinformowany o tym fakcie, związanych z tym celach i odbiorcach, którym jego dane zostaną udostępnione. Z uwagi na niedopełnienie warunków wyrażenia zgody na przetwarzanie danych osobowych wynikających z art. 4 pkt 11 RODO oraz uprzednie niepoinformowanie o udostępnieniu jego danych podmiotom trzecim, Spółka pozyskała, a następnie udostępniła dane osobowe uczestnika postepowania bez podstawy prawnej.

W dalszej części uzasadnienia decyzji PUODO odniósł się do zarzutu dotyczącego niespełnienia jego żądania w zakresie wskazania przez Spółkę odbiorców, którym udostępnione zostały jego dane i przesłanek uzasadniających to udostępnienie, udostępnienia kopii jego danych osobowych oraz żądania usunięcia jego danych.

Organ nadzorczy uznał, że doszło do naruszenia prawa w zakresie dostępu do danych, które go dotyczą, określonego w art. 15 ust. 1 lit. c RODO, bowiem Spółka posiadała żądane przez niego dane, lecz nie zrealizowała jego wniosku.

W ocenie organ nadzorczego, iSecure nie spełniła także żądania w zakresie udostępnienia kopii danych, jak i nie usunęła adresu IP uczestnika postępowania oraz sztucznie nadanego ID z cookies ze swojej bazy danych, bowiem jak wskazała nie była w stanie zidentyfikować użytkownika końcowego, którym jest

Uczestnik postępowania poinformowany został jedynie, w jaki sposób może samodzielnie usunąć pliki cookies z pamięci podręcznej swojej przeglądarki. PUODO skonstatował jednak, że z uwagi na fakt, iż stwierdził, że Spółka nie legitymuje się stosowną przesłanką uzasadniającą proces przetwarzania danych osobowych uczestnika postępowania i uznał za uzasadnione nakazanie Spółce ich usunięcia, nie może nakazać udostępnienia kopii jego danych osobowych, bowiem żądanie to dotyczyć może jedynie danych, które istnieją w zasobach Spółki.

W konkluzji PUODO stwierdził, że zebrany materiał dowodowy nie wykazał istnienia podstawy prawnej dla przetwarzania danych osobowych przez Spółkę. Należało więc uznać, że iSecure uczyniła to z naruszeniem art. 6 ust. 1 RODO. Wobec powyższego, PUODO korzystając z przysługującego mu uprawnienia określonego w art. 58 ust. 2 lit. c RODO, nakazał usunięcie danych osobowych w zakresie jego adresu IP oraz sztucznie nadanego ID z cookies. Ponadto, PUODO uznał za uzasadnione nakazanie Spółce poinformowania podmiotów, którym udostępniła dane osobowe uczestnika postępowania o ich usunięciu w oparciu o art. 19 RODO. Dodatkowo PUODO uznał za uzasadnione udzielenie Spółce upomnienia w zakresie stwierdzonego naruszenia art. 6 ust. 1, art. 15 ust. 1 lit. c oraz art. 15 ust. 3 RODO, bowiem Spółka dokonała naruszenia przepisów o ochronie danych osobowych, udostępniając podmiotom trzecim bez podstawy prawnej dane osobowe w zakresie jego adresu IP oraz sztucznie nadanego ID w cookies, nie wypełniając wobec niego obowiązku informacyjnego w zakresie wskazania informacji dotyczących właściciela domeny c t i , którym udostępniła jego dane oraz nie udostępniając uczestnikowi postępowania kopii jego danych osobowych.

Spółka zaskarżyła decyzję PUODO z 29 września 2021 r. do Wojewódzkiego Sądu Administracyjnego w Warszawie, zarzucając naruszenie:

1. art. 7, art. 77 § 1 i art. 80 K.p.a. polegające na niewyczerpującym rozpatrzeniu materiału dowodowego poprzez pominięcie dowodów przedstawionych przez skarżącą oraz dokonanie dowolnych ustaleń w przedmiocie:
   a. charakteru informacji, tj. adresu IP oraz sztucznie nadanego ID dla skarżącej (w kontekście ustalenia, czy dla skarżącej są to dane osobowe) / ustalenia, czy skarżąca ma dostęp do informacji dotyczących zidentyfikowanej lub możliwej do identyfikacji osoby fizycznej;
   b. ról podmiotów biorących udział w pozyskiwaniu ww. informacji (roli skarżącej oraz dostawców narzędzi analitycznych);
   c. ustalenia, czy skarżąca ujawniła ww. informacje wskazanym w decyzji odbiorcom;
   d. ustalenia, czy skarżąca miała faktyczną możliwość realizacji obowiązków wynikających z art. 15 RODO;
2. art. 107 § 3 k.p.a. w szczególności:
   a. poprzez takie sformułowanie uzasadnienia zaskarżanej decyzji, z którego nie wynika, na jakich dowodach PUODO oparł swoje ustalenia oraz dlaczego odmówił wiarygodności dowodom przedstawionym przez skarżącą,
   b. poprzez brak wskazania, dlaczego PUODO uznał za istotny dla rozstrzygnięcia

sprawy art. 173 Prawa telekomunikacyjnego (i dlaczego odwoływał się do problemu zgody w rozumieniu tego przepisu), skoro zakres kompetencji PUODO uniemożliwia dokonywanie ocen zgodności zachowania skarżącej z treścią tej regulacji,

c. poprzez brak wyjaśnienia, dlaczego PUODO uznał, że niewystarczające i naruszające RODO jest poinformowanie (jak to zrobiła skarżąca) o kategoriach odbiorców;

3. art. 55 ust. 1 RODO w zw. z art. 173 Prawa telekomunikacyjnego poprzez jego błędną wykładnię i przyjęcie, że PUODO jest właściwy w zakresie oceny zgodności działania skarżącej z wymogami wyrażonymi w treści art. 173 ust. 1 Prawa telekomunikacyjnego;
4. art. 174 Prawa telekomunikacyjnego poprzez jego błędną wykładnię i pominięcie - w kontekście kryteriów skuteczności zgody, o której mowa w treści tego przepisu - art. 173 ust. 2 Prawa telekomunikacyjnego;
5. art. 58 ust. 2 lit. c) i lit. d) w zw. z art. 2 ust. 1 oraz art. 4 pkt 1 RODO poprzez przyjęcie rozumienia pojęcia „danych osobowych" w sposób sprzeczny z definicją zawartą w art. 4 pkt 1 RODO, tj. bez uwzględnienia, czy dla skarżącej informacje będące przedmiotem postępowania administracyjnego mają charakter danych osobowych;
6. art. 19 RODO w zw. z art. 4 pkt 19 RODO poprzez przyjęcie, że obowiązek poinformowania odbiorców danych może obejmować także sytuację, gdy wskazane podmioty samodzielnie pozyskały dane i nie dochodzi do operacji „ujawnienia" danych, która jest elementem definicji pojęcia „odbiorcy";
7. art. 58 ust. 2 lit. c) 1 RODO poprzez nakazanie usunięcia danych osobowych, chociaż nie przedstawiono wiarygodnych dowodów wskazujących na to, że skarżąca w ogóle miała dostęp do tych danych.

Podnosząc powyższe zarzuty, Spółka wniosła o uchylenie zaskarżonej decyzji i zasądzenie kosztów postępowania według norm przepisanych.

PUODO wniósł o oddalenie skargi, podtrzymując w odpowiedzi na skargę stanowisko zawarte w uzasadnieniu zaskarżonej decyzji. W zakresie kwalifikacji adresu IP, jako danej osobowej organ nadzorczy odwołał się dodatkowo do wyroku Trybunału Sprawiedliwości Unii Europejskiej z 19 października 2016 r. w sprawie C-582/14, zaznaczając w szczególności, że Trybunał przyjął w nim obiektywne rozumienie przesłanki identyfikowalności osoby fizycznej. PUODO stwierdził też m.in., że jest właściwy do orzekania o zgodności działania Spółki z przepisami RODO, tj. oceny sposobu pozyskania przez nią zgody użytkowników końcowych na przetwarzanie ich

danych, poprzez odwołanie się do regulacji określonej w art. 173 i art. 174 Prawa telekomunikacyjnego.

Wojewódzki Sąd Administracyjny w Warszawie zważył, co następuje.

Skarga podlegała uwzględnieniu.

Zgodnie z powołanym w podstawie prawnej zaskarżonej decyzji art. 7 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 – stan prawny na dzień wydania zaskarżonej decyzji; dalej powoływana jako „uodo"), w sprawach nieuregulowanych w ustawie do postępowań administracyjnych przed Prezesem Urzędu Ochrony Danych Osobowych (dalej „PUODO"), o których mowa w rozdziałach 4-7 i 11, stosuje się ustawę z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (dalej powoływana jako „K.p.a."). Postępowaniami, o których mowa w rozdziale 7 uodo są postępowania w sprawie naruszenia przepisów o ochronie danych osobowych, do których zalicza się postępowania prowadzone w ramach realizacji przez PUODO zadań i uprawnień organu nadzorczego określonych w art. 57 i art. 58 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L. z 2016 r. Nr 119, str. 1 ze zm. – stan prawny na dzień wydania zaskarżonej decyzji; dalej powoływane jako „RODO").

Wydając zaskarżoną decyzję, PUODO skorzystał z uprawnień naprawczych przewidzianych przez art. 58 ust. 2 lit. b (udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów RODO przez operacje przetwarzania) i lit. c (nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO) RODO.

Obowiązek stosowania przepisów K.p.a. oznacza, że organ nadzorczy w postępowaniu poprzedzającym wydanie decyzji administracyjnej na podstawie art. 58 ust. 2 RODO zobowiązany jest kierować się, określonymi w K.p.a., ogólnymi zasadami postępowania oraz przepisami określającymi jego obowiązki w postępowaniu dowodowym. Stosownie do treści art. 7 K.p.a. w toku postępowania powinnością PUODO jest zatem stanie na straży praworządności i podejmowanie z urzędu lub na wniosek stron wszelkich kroków niezbędnych do dokładnego wyjaśnienia stanu faktycznego oraz do załatwienia sprawy, z uwzględnieniem interesu społecznego

i słusznego interesu obywateli. Przepis art. 77 § 1 K.p.a. obliguje zaś do wyczerpującego zebrania i rozpatrzenia całego materiału dowodowego. Zebrane przez organ administracji dowody podlegają ocenie zgodnie z zasadą swobodnej oceny dowodów, która nakazuje jako dowód dopuścić wszystko, co może przyczynić się do wyjaśnienia sprawy, a nie jest sprzeczne z prawem (art. 75 § 1 zd. 1 K.p.a.) oraz ocenić na podstawie całokształtu materiału dowodowego, czy dana okoliczność została udowodniona (art. 80 K.p.a.). Z kolei art. 11 oraz art. 107 § 1 pkt 6 i § 3 K.p.a. nakazują należycie umotywować podjęte rozstrzygnięcie.

Uzasadnienie faktyczne decyzji powinno w szczególności zawierać wskazanie faktów, które organ uznał za udowodnione, dowodów, na których się oparł, oraz przyczyn, z powodu których innym dowodom odmówił wiarygodności i mocy dowodowej, zaś uzasadnienie prawne - wyjaśnienie podstawy prawnej decyzji, z przytoczeniem przepisów prawa. Wynikającą z art. 107 § 3 K.p.a. rolą uzasadnienia jest objaśnienie toku myślenia, który doprowadził organ administracji do zastosowania lub niezastosowania przepisu prawa w konkretnej sprawie (zob. J. Borkowski [w:] Kodeks postępowania administracyjnego, Komentarz, B. Adamiak, J. Borkowski, Warszawa 2012 r., str. 441). W sferze faktów (uzasadnienia faktycznego) chodzi tu o wyjaśnienie okoliczności wskazujących na potrzebę lub konieczność wydania decyzji w danej sprawie i wobec określonych podmiotów oraz wpływu tych okoliczności na treść rozstrzygnięcia. W sferze prawa (uzasadnienia prawnego) chodzi zaś o wskazanie obowiązującej normy i jej znaczenia ustalonego w drodze wykładni (zob. J. Zimmermann, Motywy decyzji administracyjnej i jej uzasadnienie, Warszawa 1981 r., str. 118 – 122). Jak przyjmuje się w orzecznictwie Naczelnego Sądu Administracyjnego (zob. np. wyroki z 6 października 2020 r. sygn. akt I OSK 3235/18, z 24 kwietnia 2018 r. sygn. akt I OSK 1351/16 – niepublikowane; dostępne: https://orzeczenia.nsa.gov.pl), do naruszenia art. 107 § 3 K.p.a. dochodzi wtedy, gdy uzasadnienie decyzji nie zawiera wszystkich elementów wymienionych w tym przepisie, albo gdy mimo formalnej poprawności jego treść nie pozwala na skontrolowanie poprawności rozstrzygnięcia sprawy, a tym samym czyni w stopniu istotnym wątpliwym poprawność przeprowadzenia postępowania wyjaśniającego w sprawie.

Na podstawie przekazanych Sądowi akt postępowania należało stwierdzić, że PUODO naruszył powołane wyżej przepisy Kodeksu postępowania administracyjnego, a naruszenie to mogło mieć istotny wpływ na wynik sprawy. Organ nadzorczy stwierdził bowiem, że skarżąca przetwarzała bez podstawy prawnej dane osobowe [redacted]. Nie ustalił jednak uprzednio – z poszanowaniem obowiązków płynących dlań

z powołanych przepisów postępowania - czy informacje objęte rozstrzygnięciem zaskarżonej decyzji, tj. adres IP oraz sztucznie nadany ID z cookies w istocie stanowią dane osobowe uczestnika postępowania. Także uzasadnienie zaskarżonej decyzji, jakkolwiek formalnie poprawne, nie pozwala Sądowi na zweryfikowanie w realiach rozpoznanej sprawy poprawności kwalifikacji wymienionych identyfikatorów internetowych jako danych osobowych.

Wyjaśnieniu tej kluczowej dla rozstrzygnięcia sprawy kwestii poświęcono ostatni akapit szóstej strony oraz pierwszy akapit siódmej strony zaskarżonej decyzji. Najpierw PUODO prawidłowo przywołał treść art. 4 pkt 1 RODO. Zgodnie z nim, „dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Następnie organ nadzorczy trafnie odwołał się do motywu 30 RODO, w którym stwierdza się, że osobom fizycznym mogą zostać przypisane identyfikatory internetowe - takie jak adresy IP, identyfikatory plików cookie - generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób.

Dalej natomiast PODO odwołał się do wyroku Naczelnego Sądu Administracyjnego z 19 maja 2011 r. sygn. akt I OSK 1079/10, stwierdzając, że „[...] informacje, które wiążą się z określoną osobą – choćby pośrednio – niosą pewien komunikat o niej. Dlatego też informacją dotyczącą osoby jest zarówno informacja odnosząca się do niej wprost, jak i taka, która odnosi się bezpośrednio do przedmiotów czy urządzeń, ale poprzez możliwość powiązania tych przedmiotów czy urządzeń z określoną osobą pośrednio stanowi informację także o niej samej. Adres IP (Internet Protocol Address) jest unikatowym numerem przyporządkowanym urządzeniom sieci komputerowych. Jest zatem informacją dotycząca komputera, a nie konkretnej osoby fizycznej, zwłaszcza wtedy gdy możliwe jest współużyczenie jednego adresu IP przez wielu użytkowników w ramach sieci lokalnej. Tam gdzie adres IP jest na dłuższy okres czasu lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisane

jest konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową, jest to bowiem informacja umożliwiająca identyfikację konkretnej osoby fizycznej [...]".

Po przywołaniu zacytowanego fragmentu wyroku Naczelnego Sądu Administracyjnego organ nadzorczy skonstatował, że „[...] w związku z powyższym w ocenie Prezesa UODO stwierdzić należy, że zarówno adres IP Skarżącego, jak również ID plików cookies, z uwagi na uzasadnione prawdopodobieństwo zidentyfikowania Skarżącego w powiązaniu z tymi danymi, stanowią jego dane osobowe [...]".

Organ nadzorczy nie wyjaśnił, na jakiej podstawie ustalił, że istnieje „uzasadnione prawdopodobieństwo zidentyfikowania" w powiązaniu z tymi danymi, tj. adresem IP oraz ID plików cookies. Zaprezentowana natomiast przezeń - odwołująca się do wyroku Naczelnego Sądu Administracyjnego z 19 maja 2011 r. sygn. akt I OSK 1079/10 - ocena prawna, po pierwsze jednoznacznie wskazuje na to, że adres IP nie zawsze może być traktowany jako dane osobowe. Taka konstatacja - pominięta w zacytowanym przez PUODO fragmencie powołanego wyroku - została wprost wyrażona przez Naczelny Sąd Administracyjne („[...] Adres IP nie zawsze wobec tego może być traktowany jako dane osobowe w rozumieniu art. 6 ust. 1 i 2 ustawy [...]"). Po drugie, zgodnie z przyjętym w tym wyroku stanowiskiem, uznanie adresu IP za dane osobowe determinowane jest przypisaniem go na dłuższy okres lub na stałe do konkretnego urządzenia.

Wywiedziona przez PUODO w uzasadnieniu zaskarżonej decyzji kwalifikacja adresu IP jako danej osobowej odnosi się więc do tzw. stałego (statycznego) adresu IP, a nie zmiennego (dynamicznego) adresu IP. Tylko bowiem pierwszy z wymienionych jest niezmienny i umożliwia stałą identyfikację urządzenia podłączonego do sieci. Adresy dynamiczne są natomiast tymczasowe, przydzielane każdemu połączeniu z Internetem i zastępowane podczas kolejnych połączeń. Nie może zatem być mowy o ich przypisaniu - jak stwierdzono w powołanym przez PUODO wyroku Naczelnego Sądu Administracyjnego - na dłuższy czas lub na stałe do konkretnego urządzenia [zob. wyrok Trybunału Sprawiedliwości z 19 października 2016 r. w sprawie C-582/14 Breyer (pkt 36), opinia rzecznika generalnego w tej sprawie (punkty 1 – 4)].

Należy przy tym zauważyć, że dynamiczne adresy IP są najczęściej przydzielane przez dostawców dostępu do sieci (co do zasady firmy telekomunikacyjne), którzy dysponując mniejszą liczbą adresów IP niż całkowita liczba użytkowników, przydzielają na bieżąco z posiadanej puli adresy wyłącznie zakończeniom sieci korzystającym w danym momencie z połączenia, natomiast logi operatora umożliwiają stwierdzenie,

kto i kiedy posługiwał się określonym adresem IP (zob. też M. Mostowik, Ochrona danych osobowych w Internecie rzeczy w prawie UE, Warszawa 2022 r., str. 88, przypis. 186). Trzeba zatem zastrzec (o czym szerzej w dalszej części uzasadnienia), że niewątpliwie także zmienny (dynamiczny) adres IP może (ale nie w każdej sytuacji) stanowić daną osobową.

W uzasadnieniu zaskarżonej decyzji brak jednak ustaleń tak co do przyjętego w niej przez PUODO kryterium kwalifikacji adresu IP jako danej osobowej (tj. przypisania go na dłuższy czas lub na stałe do konkretnego urządzenia), jak i co do określonych w art. 4 pkt 1 w powiązaniu z motywami 26 i 30 RODO warunków uznania tego identyfikatora za daną osobową. Także z akt sprawy nie wynika, by w tym zakresie prowadzono postępowanie wyjaśniające. Na ich podstawie można stwierdzić, że już w pierwszym piśmie (z 7 lipca 2021 r.) wystosowanym do skarżącej w trybie art. 58 ust. 1 lit. a i lit. e RODO z żądaniem udzielania informacji i złożenia wyjaśnień, organ nadzorczy niejako „z góry" założył, że zarówno adres IP, jak i sztucznie nadany ID z cookies stanowią dane osobowe . Spółka w odpowiedzi z 13 sierpnia 2021 r. wyraziła stanowisko, że numer IP/ID użytkownika nie daje jej możliwości zidentyfikowania osoby odwiedzającej jej stronę internetową, a co za tym idzie, że nie przetwarzała danych osobowych uczestnika postępowania w tym zakresie, bowiem informacje te nie stanowią dla niej danych osobowych. Złożyła także do akt sprawy dokumenty mające jej zdaniem potwierdzać brak możliwości identyfikacji użytkownika strony. Mimo to, PUODO nie prowadził w toku postępowania jakichkolwiek czynności w celu ustalenia, czy informacje objęte rozstrzygnięciem zaskarżonej decyzji, tj. adres IP oraz sztucznie nadany ID z cookies w istocie są informacjami o możliwej do zidentyfikowania osobie fizycznej, tj. takiej którą można bezpośrednio lub pośrednio zidentyfikować (art. 4 pkt 1 RODO). W uzasadnieniu zaskarżonej decyzji odwołał się natomiast do wywiedzionych w wyroku Naczelnego Sądu Administracyjnego z 19 maja 2011 r. sygn. akt I OSK 1079/10 warunków kwalifikacji adresu IP jako danej osobowej, jednak nie wyjaśnił, czy w realiach przedmiotowej sprawy są one spełnione. Z akt sprawy nie wynika, czy adres IP przypisany do interfejsu sieciowego urządzenia, za pomocą którego nawiązał połączenie w celu odwiedzenia strony internetowej skarżącej, był adresem stałym, czy zmiennym.

Niewyjaśnienie tej istotnej, w świetle przyjętych w zaskarżonej decyzji kryteriów uznania adresu IP za daną osobową, okoliczności (stałego lub zmiennego charakteru adresu IP interfejsu sieciowego urządzenia, z którego korzystał , nie mogłoby mieć istotnego wpływu na wynik sprawy, gdyby dopuszczalne w świetle przepisów

RODO było przyjęcie, że adres IP jest daną osobową w rozumieniu art. 4 pkt 1 RODO niezależnie od tego, czy jest adresem stałym, czy zmiennym oraz niezależnie od tego, w czyim znajduje się posiadaniu oraz jakie możliwości posiada dysponent tej informacji w celu dokonania identyfikacji. Taki wniosek nie znajduje jednak oparcia ani w przepisach RODO, ani w stanowisku Trybunału Sprawiedliwości Unii Europejskiej odnoszącym się wprawdzie do dyrektywy Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE. L. z 1995 r. Nr 281, str. 31 ze zm.), które jednak w istotnej dla przedmiotowej sprawy części zachowuje aktualność na tle przepisów RODO.

Przede wszystkim należy zauważyć, że RODO nie rozstrzyga, czy same identyfikatory internetowe, takie jak adresy IP, czy identyfikatory plików cookies powinny zawsze być traktowane jako dane osobowe, czy jako jeden z czynników („śladów"), które mogą pozwolić na identyfikację osoby fizycznej. W powołanym wyżej motywie 30 stwierdza się bowiem, że ich wykorzystanie „(...) może (...) skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób [...]". W art. 4 pkt 1 RODO stanowi zaś, że możliwa do zidentyfikowania osoba fizyczna, to taka którą można bezpośrednio lub pośrednio zidentyfikować w szczególności na podstawie identyfikatora internetowego.

Swoisty test możliwości identyfikacji osoby fizycznej przewidziano w motywie 26 RODO, który wskazuje, że „[...] aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane (ang. wers. jęz.: *all the means reasonably likely to be used* – przyp. Sądu) przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany (ang. wers. jęz.: *whether means are reasonably likely to be used* – przyp. Sądu) do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny [...]".

W świetle powyższego nie ma podstaw, by uznać, że adres IP – niezależnie od tego, czy jest adresem stałym (statycznym), czy zmiennym (dynamicznym) oraz

niezależnie od tego, kto jest jego dysponentem i jakie istnieją możliwości wykorzystania go w celu identyfikacji osoby fizycznej, należy zawsze traktować jako daną osobową. Ten sam wniosek dotyczy identyfikatorów plików cookies. Odpowiadając na pytanie, czy określone identyfikatory internetowe stanowią dane osobowe należy bowiem wziąć pod uwagę „wszelkie rozsądnie prawdopodobne sposoby (...), w stosunku do których istnieje uzasadnione prawdopodobieństwo", że zostaną wykorzystane przez administratora lub inną osobę w celu zidentyfikowania osoby fizycznej. Miarą uzasadnionego prawdopodobieństwa wykorzystania danego sposobu identyfikacji (np. z wykorzystaniem adresu IP lub identyfikatora pliku cookie) powinny być zaś „wszelkie obiektywne czynniki", do których prawodawca unijny w szczególności zalicza „koszt i czas potrzebne do zidentyfikowania" osoby fizycznej, „technologię dostępną w momencie przetwarzania danych" i „postęp technologiczny". Nie powinna mieć przy tym rozstrzygającego znaczenia możliwość dokonania samoidentyfikacji przez osobę, której dane dotyczą.

Potwierdzenie obowiązku stosowania tzw. „klauzuli rozsądku" w procesie kwalifikacji identyfikatora internetowego w postaci zmiennego adresu IP jako danej osobowej stanowi wyrok Trybunału Sprawiedliwości Unii Europejskiej z 19 października 2016 r. w sprawie C-582/14 Breyer.

W wyroku tym (pkt 42) odwołano się do motywu 26 dyrektywy 95/46 wskazując, że „(...) w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może, racjonalnie rzecz biorąc, posłużyć się (ang. wers. jęz.: *all the means likely reasonably to be used* – przyp. Sądu) administrator danych lub inna osoba w celu zidentyfikowania owej osoby [...]". Następnie natomiast stwierdzono (pkt 43), że „[...] w zakresie, w jakim wskazany wyżej motyw odnosi się do sposobów, jakimi mogą, racjonalnie rzecz biorąc, posłużyć się zarówno administrator danych, jak i *inna osoba*, brzmienie tego motywu sugeruje, że aby dane mogły zostać uznane za *dane osobowe* w rozumieniu art. 2 lit. a) wspomnianej dyrektywy, nie jest wymagane, by wszystkie informacje umożliwiające identyfikację osoby, której dane dotyczą, musiały znajdować się w rękach tylko jednej osoby [...]".

Jak skonstatował Trybunał (pkt 44), „[...] nie wydaje się zatem, by okoliczność, że dodatkowe informacje konieczne do identyfikacji użytkownika strony internetowej są w posiadaniu nie dostawcy usług medialnych online, lecz dostawcy dostępu do Internetu dla tego użytkownika, mogła wykluczać to, iż dynamiczne adresy IP zarejestrowane przez dostawcę usług medialnych online stanowią dla niego dane osobowe w rozumieniu art. 2 lit. a) dyrektywy 95/46 [...]". Trybunał zaznaczył jednak

również, że „[...] należy (...) ustalić, czy możliwość połączenia dynamicznego adresu IP z owymi dodatkowymi informacjami będącymi w posiadaniu tego dostawcy dostępu do Internetu stanowi sposób, który może, racjonalnie rzecz biorąc, zostać zastosowany w celu zidentyfikowania osoby, której dane dotyczą [...]". Odwołując się do opinii rzecznika generalnego, Trybunał wskazał, że „(...) nie miałoby to miejsca w przypadku, gdyby identyfikacja osoby, której dane dotyczą, była zakazana prawem lub niewykonalna w praktyce, przykładowo z powodu okoliczności, że wiąże się ona z nadmiernym nakładem czasu, kosztów i pracy ludzkiej, tak że ryzyko identyfikacji wydaje się w rzeczywistości znikome [...]".

Uwzględniając opisane wyżej warunki zakwalifikowania dynamicznego adresu IP jako danej osobowej, Trybunał stwierdził następnie (punkty 47 – 49), że „(...) jakkolwiek sąd odsyłający wyjaśnia w swoim postanowieniu odsyłającym, że prawo niemieckie nie pozwala dostawcy dostępu do Internetu przekazywać bezpośrednio dostawcy usług medialnych online dodatkowych informacji koniecznych do identyfikacji osoby, której dane dotyczą, wydaje się jednak – z zastrzeżeniem konieczności zweryfikowania tego przez ten sąd – że istnieją środki prawne umożliwiające dostawcy usług medialnych online zwrócenie się do właściwego organu, aby podjął on konieczne działania w celu uzyskania tych informacji od dostawcy dostępu do Internetu oraz w celu wszczęcia ścigania karnego [...]". Trybunał przyjął zatem, iż „(...) wydaje się, że dostawca usług medialnych online dysponuje środkami, którymi może, racjonalnie rzecz biorąc, posłużyć się w celu zidentyfikowania – z pomocą innych osób, czyli właściwego organu i dostawcy dostępu do Internetu – osoby, której dane dotyczą, na podstawie przechowywanych adresów IP [...]".

Mając na względzie całość przedstawionych rozważań, Trybunał skonstatował, że „(...) dynamiczny adres IP zarejestrowany przez dostawcę usług medialnych online przy okazji przeglądania przez daną osobę strony internetowej, którą dostawca ten udostępnia publicznie, stanowi wobec tego dostawcy dane osobowe w rozumieniu tego przepisu, w sytuacji gdy dysponuje on środkami prawnymi umożliwiającymi mu zidentyfikowanie osoby, której dane dotyczą, dzięki dodatkowym informacjom, jakimi dysponuje dostawca dostępu do Internetu dla tej osoby [...]".

Opisany wyrok Trybunału Sprawiedliwości Unii Europejskiej został powołany w odpowiedzi PUODO na skargę, w której stwierdzono, że Trybunał przyjął w nim tzw. obiektywne rozumienie przesłanki identyfikalności osoby fizycznej uznając, że nie jest wymagane, by wszystkie informacje umożliwiające identyfikację osoby, której dane dotyczą, musiały znajdować się w rękach tylko jednej osoby i w konsekwencji uznając

dynamiczny adres IP za dane osobowe.

Mając powyższe na uwadze, po pierwsze należy podkreślić, że kontroli Sądu podlegała zaskarżona decyzja, a nie stanowisko strony postępowania wyrażone w piśmie złożonym w sprawie. Jak natomiast wywiedziono powyżej, wyjaśnienie podstawy prawnej zaskarżonej decyzji w zakresie kwalifikacji objętych jej rozstrzygnięciem informacji (adresu IP i sztucznie nadanego IP z cookies) jako danych osobowych ogranicza się do przywołania treści art. 4 pkt 1 i motywu 30 RODO, fragmentu uzasadnienia wyroku Naczelnego Sądu Administracyjnego z 19 maja 2011 r. sygn. akt I OSK 1079/10 i konstatacji, że „zarówno adres IP skarżącego jak również ID plików cookies, z uwagi na uzasadnione prawdopodobieństwo zidentyfikowania skarżącego w powiązaniu z tymi danymi, stanowią jego dane osobowe".

Po drugie, fakt, że w wyroku w sprawie C-584/14 Trybunał przyjął tzw. obiektywne podejście do przesłanki identyfikowalności osoby fizycznej nie oznacza, iż stwierdził, że dynamiczny adres IP, niezależnie od okoliczności konkretnej sprawy, zawsze stanowi wobec dostawcy usług medialnych (np. prowadzącego stronę internetową) dane osobowe. Z wyroku tego jednoznacznie wynika, że Trybunał, odpowiadając na pytanie sądu odsyłającego, oparł się na założeniu tego sądu, zgodnie z którym, dane obejmujące dynamiczny adres IP oraz datę i godzinę przeglądania strony internetowej z tego adresu IP, zarejestrowane przez dostawcę usług medialnych online, nie dają same w sobie temu dostawcy możliwości zidentyfikowania użytkownika, który przeglądał tę stronę internetową w trakcie danej sesji, a z drugiej strony dostawca dostępu do Internetu dysponuje dodatkowymi informacjami, które w połączeniu z tym adresem IP umożliwiają identyfikację danego użytkownika. Trybunał oparł się jednak także na założeniu (z zastrzeżeniem konieczności zweryfikowania tego przez sąd krajowy), że w prawie niemieckim istnieją środki prawne umożliwiające dostawcy usług medialnych online (w tej sprawie był do Rząd Republiki Federalnej Niemiec) zwrócenia się do właściwego organu, aby podjął on konieczne działania w celu uzyskania dodatkowych informacji od dostawcy dostępu do Internetu oraz w celu wszczęcia ścigania karnego. Jak wynika z wyroku (pkt 13 i pkt 14), aby chronić się przed atakami i umożliwić ściganie na drodze karnej „piratów", w przypadku stron internetowych niemieckich służb federalnych, każde wejście na stronę jest rejestrowane w pliku logów. Po zakończeniu danej sesji w danych tych przechowuje się nazwę konsultowanych danych lub strony, pojęcia wpisane w polach wyszukiwania, dzień i godzinę konsultacji, ilość przesłanych danych, informację, czy konsultacja się powiodła, oraz adres IP komputera, za pomocą którego przeglądano określone dane lub strony.

W uzasadnieniu zaskarżonej decyzji organ w ogóle nie odnosił się do kwestii możliwości prawnych zwrócenia się przez skarżącą do właściwego organu w celu uzyskania od dostawcy dostępu do Internetu informacji pozwalających - w połączeniu z adresem IP – na identyfikację osoby, której skarga wszczęła postępowanie przed PUODO. Z akt sprawy wynika, że organ nadzorczy - pomimo podnoszonej w toku postępowania argumentacji skarżącej wskazującej na brak możliwości identyfikacji - nie rozważał też tej kwestii w toku postępowania.

W świetle określonych w motywie 26 RODO kryteriów oceny danego sposobu identyfikacji jako „rozsądnie prawdopodobnego do wykorzystania", należy natomiast brać pod uwagę „wszelkie obiektywne czynniki", do których przykładowo zaliczono koszt i czas potrzebne do jej zidentyfikowania. Nie ma więc podstaw, by stwierdzone przez Trybunał w wyroku w sprawie C-582/14 „rozsądne prawdopodobieństwo" zidentyfikowania osoby fizycznej (na podstawie zmiennego adresu IP w powiązaniu z dodatkowymi informacjami, jakimi dysponuje dostawca dostępu do Internetu dla tej osoby) - przez będący dostawcą usługi internetowej (prowadzącym stronę internetową) Rząd Republiki Federalnej Niemiec, który gromadził informacje o tych adresach w celu wszczęcia ścigania karnego wobec osób dokonujących „ataków" na strony internetowe rządu federalnego – „przejmować" *a limine* w każdym innym przypadku dysponowania przez dostawcę usługi internetowej zmiennym adresem IP użytkownika Internetu.

Niewątpliwie okoliczność, że dodatkowe informecje konieczne do identyfikacji użytkownika strony internetowej są w posiadaniu nie dostawcy usług medialnych online, lecz dostawcy dostępu do Internetu dla tego użytkownika, nie wyklucza uznania zmiennego adresu IP zarejestrowanego przez dostawcę usług medialnych online za dane osobowe. Uznanie przez Trybunał, że ustalenie tożsamości osoby fizycznej na podstawie zmiennego adresu IP (posiadanego przez dostawcę usługi internetowej) oraz innych danych (posiadanych przez dostawcę dostępu do Internetu) było „rozsądnie prawdopodobne do wykorzystania" w sprawie C-582/14 nie oznacza jednak, że stwierdził on, iż takie - rozsądne - prawdopodobieństwo istnieje zawsze, niezależnie od tego, kto dysponuje tymi informacjami, a także od tego, jakie „obiektywnie istniejące czynniki" (np. koszt i czas potrzebne do zidentyfikowania, dostępne środki techniczne – motyw 26 RODO, czy też prawna dopuszczalność zaangażowania dostawcy dostępu do Internetu w proces identyfikacji) wpływają na możliwość ich powiązania w celu identyfikacji. Jak już wskazano, wszystkie te okoliczności pozostały poza zakresem postępowania wyjaśniającego poprzedzającego wydanie zaskarżonej decyzji.

Rozstrzygnięciem zaskarżonej decyzji objęto nie tylko adres IP, ale także „sztucznie nadany ID z cookies". Konstatację, że „zarówno adres IP Skarżącego, jak również ID plików cookies, z uwagi na uzasadnione prawdopodobieństwo zidentyfikowania Skarżącego w powiązaniu z tymi danymi, stanowią jego dane osobowe" poprzedzono jednak wyjaśnieniem podstawy prawnej decyzji w zakresie kwalifikacji jako danej osobowej (w świetle art. 4 pkt 1 i motywu 30 RODO) wyłącznie adresu IP. Na stronie 7 zaskarżonej decyzji PUODO przywołał wprawdzie pkt 67 wyroku Trybunału Sprawiedliwości Unii Europejskiej z 1 października 2019 r. w sprawie C-673/17 – stwierdzając, że Trybunał wskazał, iż „(...) instalowanie plików cookie, o którym mowa w postępowaniu głównym, wiąże się z przetwarzaniem danych osobowych [...]". Zacytowane stwierdzenie zostało jednak oparte na ustaleniach zawartych w punkcie 45 wyroku Trybunału, gdzie stwierdzono, że „(...) pliki cookie, które mogą być instalowane na urządzeniu końcowym użytkownika uczestniczącego w loterii promocyjnej zorganizowanej przez spółkę zawierają numer przypisany do danych rejestracyjnych tego użytkownika, który w formularzu uczestnictwa w tej grze musi wpisać swoje imię i nazwisko oraz adres. Sąd odsyłający dodaje, że skojarzenie tego numeru z tymi danymi powoduje personalizację danych przechowywanych przez pliki cookie, gdy użytkownik korzysta z Internetu, wobec czego zbieranie tych danych za pomocą plików cookie jest przetwarzaniem danych osobowych [...]".

W okolicznościach sprawy zakończonej zaskarżoną decyzją nie doszło do sytuacji, w której wypełnił jakikolwiek formularz na stronie internetowej skarżącej, a tym bardziej taki, w którym podałby swoje imię, nazwisko lub adres. Skarżąca w piśmie z 13 sierpnia 2021 r. wyjaśniała natomiast, że właściciel domeny to dostawca oprogramowania dla Spółki służącego do przesyłania wiadomości on-line podczas wizyty na stronie lub zamówienia rozmowy telefonicznej, oraz że w przypadku, gdy nie zostanie rozpoczęty czat, żadne informacje poza adresem IP odwiedzającego stronę nie są przekazywane temu dostawcy. Ponadto, jak utrzymywała iSecure, wszystkie inne domeny wymienione przez i wynikają z wykorzystywania plików cookies analitycznych na stronie Spółki. Spółka zaznaczała, że wysyłane jest jedynie zapytanie dotyczące cookie ID, a nie historia przeglądania. Wywodziła też, że za pomocą unikalnego identyfikatora, który został przekazany za pomocą cookies analitycznego, nie można dokonać identyfikacji użytkownika końcowego, którym jest uczestnik postępowania.

W tych okolicznościach zaczerpnięte z wyroku w sprawie C-673/17

stwierdzenie, że „instalowanie plików cookie, o których mowa w postępowaniu głównym, wiąże się z przetwarzaniem danych osobowych" nie może być uznane za prawidłowe wyjaśnienie podstawy prawnej decyzji z zakresie, w jakim ID plików cookies zostały zakwalifikowane jako dane osobowe

Sąd podkreśla, że miał na uwadze, iż zidentyfikowanie osoby fizycznej nie musi polegać na określeniu jej imienia i nazwiska. Konstatacja ta jest szczególnie istotna w środowisku cyfrowym, w którym identyfikacja sprowadza się do oznaczenia danego użytkownika w celu wywierania na niego określonego wpływu (zob. [w:] Ochrona Danych Osobowych [red.] Warszawa 2020 r., str. 81). Identyfikacja osoby nie wymaga zatem znajomości jej imienia lub nazwiska, wymaga natomiast znajomości pewnych unikalnych cech tej osoby, które odróżniają ją od innych. W ten sposób należy rozumieć zwrot "można zidentyfikować" – nie tylko jako możliwość odniesienia konkretnej informacji do konkretnej osoby, lecz jako możliwość wskazania tej osoby, rozumianego jako faktyczne wyodrębnienie jej spośród innych osób (zob. . [w:] Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, Komentarz [red.] Warszawa 2018 r., str. 181).

Z uzasadnienia zaskarżonej decyzji nie wynika jednak, by PUODO postrzegał możliwość identyfikacji uczestnika postępowania w środowisku cyfrowym, jako użytkownika Internetu o określonych cechach, a nie jako osobę fizyczną możliwą do zidentyfikowania z imienia i nazwiska. Świadczy o tym odwołanie się do wyroku Naczelnego Sądu Administracyjnego z 19 maja 2011 r. sygn. akt I OSK 1079/10 i wyroku Trybunału Sprawiedliwości Unii Europejskiej z 1 października 2019 r. w sprawie C-673/17, jak również konstatacja organu nadzorczego, że do zidentyfikowania może dojść „w powiązaniu z tymi danymi". W sprawach, których dotyczą oba powołane orzeczenia odnoszono się do możliwości identyfikacji osób fizycznych z wykorzystaniem adresu IP (wyrok Naczelnego Sądu Administracyjnego) i identyfikatorów plików cookie (wyrok Trybunału Sprawiedliwości Unii Europejskiej) poprzez oznaczenie jej z imienia i nazwiska. Na podstawie uzasadnienia zaskarżonej decyzji, twierdzenia organu nadzorczego, że adres IP i ID plików cookies stanowią dane osobowe z uwagi na wysokie prawdopodobieństwo zidentyfikowania w powiązaniu z tymi danymi, nie można więc rozumieć w ten sposób, że w ocenie organu nadzorczego, np. poprzez dane powiązane z plikami cookies zapisanymi w pamięci przeglądarki informujące o oprogramowaniu użytkownika, jego zachowaniach w sieci, zainteresowaniach, czy inne metadane związane z korzystaniem z usługi

internetowej, możliwe jest odróżnienie od innych osób, bez konieczności znajomości jego imienia i nazwiska. Jak już nadmieniono – poza przytoczeniem art. 4 pkt 1 i motywu 30 RODO, które z przedstawionych wyżej względów nie rozstrzygają jednoznacznie, że identyfikatory plików cookies powinny być zawsze traktowane jako dane osobowe – PUODO nie odnosił się do kwestii kwalifikacji ID plików cookies (czy to samodzielnie, czy to w połączeniu z innymi unikatowymi identyfikatorami i innymi informacjami), jako danych osobowych w okolicznościach przedmiotowej sprawy, w szczególności do podnoszonych przez skarżącą kwestii dotyczących rodzaju wykorzystywanych plików cookie. Sąd administracyjny, dokonując kontroli decyzji administracyjnej, nie jest natomiast uprawniony do wyręczania organu administracji w należytym wyjaśnieniu okoliczności faktycznych istotnych dla rozstrzygnięcia sprawy.

Z powyższych względów należało stwierdzić, że w sprawie zakończonej zaskarżoną decyzją nie wyjaśniono należycie okoliczności zasadniczej dla jej rozstrzygnięcia, tj. kwalifikacji adresu IP interfejsu sieciowego urządzenia, z którego korzystał oraz identyfikatorów plików cookie, które zostały zapisane na urządzeniu, z którego korzystał, jako jego danych osobowych. Jak już wskazano, uchybienie to jest równoznaczne z naruszeniem art. 7, art. 77 § 1, art. 80 i art. 107 § 3 K.p.a., które mogło mieć istotny wpływ na wynik sprawy. Prawidłowe ustalenie tej podstawowej w sprawie kwestii determinuje bowiem dopuszczalność udzielania skarżącej upomnień i nałożenia na nią obowiązków określonych w zaskarżonej decyzji. W aktualnym stanie sprawy nie ma zatem podstaw do oceny zasadności podnoszonych przez skarżącą w ramach zarzutów naruszenia przepisów postępowania kwestii dotyczących niewyjaśnienia przez PUODO ról podmiotów biorących udział w procesie przetwarzania danych, ani możliwości realizacji przez skarżącą obowiązku określonego w art. 15 RODO.

Z uwagi na podstawiony przez Spółkę zarzut naruszenia art. 55 ust. 1 RODO w zw. z art. 173 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576 – stan prawny na dzień wydania zaskarżonej decyzji; dalej powoływana jako „Prawo telekomunikacyjne") - zastrzegając, że w ponownie przeprowadzonym postępowaniu, w pierwszej kolejności obowiązkiem PUODO będzie wyjaśnienie, czy adres IP interfejsu sieciowego urządzenia, z którego korzystał przeglądając stronę internetową skarżącej, a także ID plików cookie zapisanych na jego urządzeniu w czasie korzystania z tej stronny, stanowią jego dane osobowe - Sąd za zasadne uznał zaznaczenie, że jeżeli przetwarzanie danych osobowych jest objęte zarówno zakresem przedmiotowym RODO, jak i dyrektywy 2002/58/WE

Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. UE. L. z 2002 r. Nr 201, str. 37 ze zm.), organy ochrony danych posiadają właściwość do przeprowadzenia kontroli podzbiorów przetwarzania podlegających przepisom krajowym transponującym dyrektywę o prywatności i łączności elektronicznej tylko wtedy, gdy prawo krajowe stanowi, że należy to do ich właściwości. Niemniej jednak, sam fakt, że podzbiór przetwarzania wchodzi w zakres dyrektywy o prywatności i łączności elektronicznej nie ogranicza właściwości organów ochrony danych na podstawie RODO. Sąd podziela w tej kwestii stanowisko wyrażone w opinii Rady do Spraw Ochrony Danych Osobowych z 12 marca 2019 r. nr 5/2019 w sprawie wzajemnej zależności między dyrektywą o prywatności i łączności elektronicznej a RODO, w szczególności w zakresie właściwości, zadań i uprawnień organów ochrony danych (str. 22 i str. 26).

Aktem prawnym transponującymi dyrektywę o prywatności i łączności elektronicznej do krajowego porządku prawnego jest Prawo telekomunikacyjne. Nie przewidziano w nim właściwości PUODO do oceny prawidłowości przechowywania informacji lub uzyskiwania dostępu do informacji już przechowywanej w telekomunikacyjnym urządzeniu końcowym abonenta lub użytkownika końcowego (art. 5 ust. 3 dyrektywy i art. 173 ust. 1 Prawa telekomunikacyjnego). Stosownie do treści art. 209 ust. 1 pkt 25 i pkt 27 Prawa telekomunikacyjnego, kto: nie wypełnia obowiązków uzyskania zgody abonenta lub użytkownika końcowego, o której mowa m.in. w art. 174 (pkt 25), a także niezgodnie z przepisami art. 173 przechowuje informacje w urządzeniach końcowych abonenta lub użytkownika końcowego lub korzysta z informacji zgromadzonych w tych urządzeniach (pkt 27), podlega karze pieniężnej. Wedle zaś art. 209 ust. 1^1 pkt 2 Prawa telekomunikacyjnego, Prezes UKE, jeżeli przemawia za tym charakter lub zakres naruszenia, może nałożyć karę pieniężną na podmiot, który nie wypełnia obowiązków uzyskania zgody abonenta lub użytkownika końcowego, o których mowa w art. 173. Jak wynika z art. 210 ust. 1 Prawa telekomunikacyjnego, kary pieniężne, o których mowa w art. 209 ust. 1 i 1^1, nakłada Prezes UKE, w drodze decyzji.

Z powyższego wynika, że zapewnienie zgodności z prawem przechowywania informacji w urządzeniach końcowych abonenta lub użytkownika końcowego lub korzystania z informacji zgromadzonych w tych urządzeniach należy do właściwości Prezesa UKE.

Jak jednak dostrzeżono w powołanej wyżej opinii Rady do Spraw Ochrony Danych Osobowych (str. 24), „(...) w przypadku, gdy dla różnych instrumentów prawnych właściwe są różne organy, powinny one zapewnić, aby egzekwowanie obydwu instrumentów było spójne, między innymi, aby uniknąć naruszenia zasady *non bis in idem*, kiedy naruszenia przepisów RODO oraz dyrektywy o prywatności i łączności elektronicznej, które wystąpiły w kontekście jednej z czynności przetwarzania, są ściśle ze sobą powiązane [...]".

Mając powyższe na uwadze, należy zauważyć, że Trybunał Sprawiedliwości Unii Europejskiej w wyroku z 29 lipca 2019 r. w sprawie C-40/17 Fashion ID stwierdził, że „[...] operatora witryny internetowej, (...), który umieszcza we wspomnianej witrynie wtyczkę społecznościową umożliwiającą przeglądarce osoby odwiedzającej tę witrynę pobieranie treści od dostawcy wspomnianej wtyczki i przekazywanie w tym celu temu dostawcy danych osobowych osoby odwiedzającej, można uznać za administratora danych w rozumieniu art. 2 lit. d) dyrektywy 95/46. Jego odpowiedzialność jest jednak ograniczona do operacji lub do zestawu operacji przetwarzania danych osobowych, której lub których cele i sposoby rzeczywiście on określa, mianowicie gromadzenia rozpatrywanych danych i ich ujawniania poprzez transmisję [...]".

Zastrzegając, że: (1) w okolicznościach sprawy zakończonej zaskarżoną decyzją kwestia kwalifikacji adresu IP oraz identyfikatorów plików cookies jako danych osobowych wymaga wyjaśnienia; (2) podmiotem administrującym stroną internetową w sprawie C-40/17 Fashion ID była spółka prowadząca sprzedaż online, co niewątpliwie wpływa na zakres gromadzonych danych o użytkownikach tej strony; (3) informacje przekazywane dostawcy wtyczki internetowej obejmowały zarówno adres IP, jak i inne dane – niekoniecznie ograniczające się do informacji przechowywanych w urządzeniu końcowym (zob. pkt 26 i pkt 91 wyroku); zaś (4) Trybunał przyjął w tej sprawie za sądem odsyłającym, że dane przekazywane dostawcy wtyczki stanowią dane osobowe (zob. pkt 91 wyroku); (5) należy stwierdzić, że w świetle powołanego stanowiska Trybunału, które należy uznać za aktualne w obecnym stanie prawnym, operatora witryny internetowej, który umieszcza na stronie internetowej kod programu, który inicjuje żądanie przez przeglądarkę użytkownika treści od osoby trzeciej i przekazywanie danych osobowych osobie trzeciej, można uznać za administratora danych, nawet jeśli nie ma on wpływu (po wpisaniu kodu takiego programu) na to przetwarzanie. W przypadku niewpisania owego kodu nie doszłoby bowiem do udostępnienia. Okoliczność, że operator witryny internetowej sam nie ma dostępu do danych osobowych gromadzonych i przekazywanych do dostawcy programu, którego

kod wpisano do tej witryny, nie stoi na przeszkodzie, by przysługiwał mu przymiot administratora danych w rozumieniu art. 4 pkt 7 RODO (zob. pkt 82 wyroku w sprawie Fashion ID). Odpowiedzialność operatora witryny internetowej ogranicza się jednak do operacji lub zestawu operacji, których cele i sposoby rzeczywiście określa, tj. do zbierania danych osobowych i ich ujawnienia przez przesłanie osobie trzeciej będącej dostawcą programu, którego kod wstawiono do strony internetowej.

Jeżeli zatem w okolicznościach przedmiotowej sprawy należałoby uznać adres IP i ID. plików cookies za dane osobowe, a ich przekazanie właścicielom domen wskazanych w skardze z 28 czerwca 2021 r. byłoby skutkiem umieszczenia na stronie internetowej Spółki kodów programów dostarczanych przez te podmioty na potrzeby skarżącej (co również wymagałoby wyjaśnienia w toku postępowania), to doszłoby do sytuacji analogicznej do będącej przedmiotem analizy Trybunału w sprawie w sprawie C-40/17 I ID. Miałoby bowiem miejsce zbieranie danych osobowych i ich ujawnianie przez przesłanie osobie trzeciej będącej dostawcą programu, którego kod wstawiono do strony internetowej. W tych okolicznościach – choć przetwarzanie danych osobowych związane byłoby z umieszczeniem informacji w urządzeniach końcowych lub korzystaniem z informacji zgromadzonych w tych urządzeniach – właściwość organu ochrony danych osobowych nie budzi wątpliwości, a zgoda na przetwarzanie danych osobowych powinna spełniać warunki, o których mowa w art. 4 pkt 11 i motywie 32 RODO. PUODO pozostaje bowiem w pełni właściwy do oceny zgodności z prawem wszelkich innych operacji przetwarzania danych osobowych odbywających się w następstwie przechowywania informacji lub uzyskania dostępu do informacji przechowywanej na urządzeniu końcowym (zob. str. 23 powołanej wyżej opinii Rady do Spraw Ochrony Danych Osobowych).

W ponownie przeprowadzonym postępowaniu PUODO podejmie czynności mające na celu ustalenie, czy w okolicznościach przedmiotowej sprawy informacje objęte rozstrzygnięciem zaskarżonej decyzji, tj. adres IP oraz sztucznie nadany ID z cookies w istocie stanowią dane osobowe , tj. dane o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Organ nadzorczy weźmie pod uwagę, iż przepisy RODO nie rozstrzygają, że identyfikatory internetowe, takie jak adresy IP, czy identyfikatory plików cookies powinny zawsze być traktowane jako dane osobowe, oraz że w świetle określonych w motywie 26 RODO kryteriów oceny danego sposobu identyfikacji jako „rozsądnie prawdopodobnego do wykorzystania" w celu identyfikacji osoby fizycznej, należy wziąć pod uwagę „wszelkie obiektywne czynniki", jak np. koszt i czas potrzebne do zidentyfikowania, dostępne środki techniczne, czy możliwości

prawne. W razie potrzeby, PUODO wezwie strony postępowania do złożenia dodatkowych wyjaśnień i dokumentów lub przeprowadzi inne niezbędne dowody. Uzasadnienie nowo wydanej decyzji powinno zawierać w szczególności wyczerpujące wyjaśnienie podstawy prawnej rozstrzygnięcia w zakresie kwalifikacji objętych nią informacji, jako danych osobowych lub braku podstaw do takiej kwalifikacji. Organ nadzorczy odniesie przyjęte w uzasadnieniu decyzji kryteria kwalifikacji adresu IP i identyfikatorów plików cookies jako danych osobowych do materiału dowodowego zgromadzonego w toku postępowania.

W tym stanie rzeczy, na podstawie art. 145 § 1 pkt 1 lit. c ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. z 2022 r. poz. 329 ze zm.), Wojewódzki Sąd Administracyjny w Warszawie uchylił zaskarżoną decyzję.

O zwrocie kosztów postępowania Sąd orzekł na podstawie art. 200 w zw. z art. 205 § 2 P.p.s.a. Objęły one uiszczony wpis od skargi (200 zł), wydatek w postaci opłaty skarbowej za złożenie dokumentu stwierdzającego udzielenie pełnomocnictwa (17 zł) oraz wynagrodzenie radcy prawnego (480 zł) ustalone zgodnie z § 14 ust. 1 pkt 1 lit. c) rozporządzenia Ministra Sprawiedliwości z dnia 22 października 2015 r. w sprawie opłat za czynności radców prawnych (Dz. U. z 2018 r. poz. 265).

Na oryginale właściwe podpisy
Za zgodność z oryginałem
starszy specjalista