Fragment

Ochrona danych osobowych w sektorze publicznym + wzory do pobrania

Paweł Litwiński, Kamil Pakalski, Magdalena Szczytko-Sołtysiak

Rozdział I. Dane osobowe, pseudonimizacja i anonimizacja

1. Pojęcie danych osobowych

Czym są dane osobowe? To z pozoru proste pytanie, bo pojęcie danych osobowych nie dość, że zostało zdefiniowane w art. 4 pkt 1 RODO, to jeszcze ta definicja w zasadzie nie różni się od tej znanej jeszcze z przepisów OchrDanychU97. Ale w przypadku pojęcia danych osobowych doskonale sprawdza się powiedzenie, że pozory mylą.

Czym więc są dane osobowe? Dane osobowe to:
1) informacje,
2) o osobie fizycznej,
3) która to osoba jest zidentyfikowana lub możliwa do zidentyfikowania.

Czym jest informacja? W pewnym uproszczeniu informacją nazwiemy to wszystko, co zwiększa naszą wiedzę na temat tego, do czego (tutaj: do kogo) ta informacja się odnosi. Będzie więc tak, że każda informacja, niezależnie od sposobu i formy jej wyrażenia, podlegać może ocenie z punktu widzenia pojęcia danych osobowych i każda informacja może zostać uznana za informację o charakterze osobowym[1]. Taką informacją może być dźwięk, obraz, zdjęcie, znaki językowe, dane biometryczne itp. – to po prostu komunikaty wyrażone i zapisane w jakikolwiek sposób, niezależnie od sposobu, zakresu i swobody ich udostępniania, jak i niezależnie od sposobu ich pozyskania. Mogą to być zarówno informacje, które identyfikują osobę (m.in. imię, nazwisko, adres, numer identyfikacyjny, wizerunek), jak też informacje, które odnoszą się do jej cech lub statusu osobistego (m.in. stan cywilny, obywatelstwo, stan zdrowia, wykształcenie, karalność) lub

[1] *P. Barta*, *M. Kawecki*, *P. Litwiński*, (w:) Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, red. *P. Litwiński*, Warszawa 2021, s. 81.

informacje o charakterze rzeczowym (m.in. wysokość wynagrodzenia, stan posiadania, stosunki własnościowe)[2].

Ważne

Charakter danych osobowych – potencjalnie – może mieć każda informacja. Żadnej nie można z góry wykluczyć, ani żadnej z góry nie można przyznać charakteru danych osobowych.

Informacja może zostać uznana za mającą charakter danych osobowych tylko wtedy, gdy dotyczy „osoby fizycznej" – od jej narodzin aż do śmierci. Potwierdza tę regułę motyw 27 preambuły do RODO, zgodnie z którym RODO nie ma zastosowania do danych osobowych osób zmarłych, a państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych. Ponieważ w polskim porządku prawnym nie ma ustawy regulującej zasady przetwarzania danych osobowych osób zmarłych, informacje takie nie podlegają ochronie na podstawie przepisów RODO.

Podmioty publiczne, realizując swoje zadania, mogą przetwarzać dane osobowe dzieci. Przykładem takich projektów są realizowane np.:

1) program „Mama 4+" (MRiPS) skierowany do osób, które wychowują co najmniej czwórkę dzieci, nie mogły podjąć się pracy zarobkowej lub z niej zrezygnowały, a obecnie znajdują się w ciężkiej sytuacji ekonomicznej[3];
2) prowadzenie ewidencji małoletnich obywateli Ukrainy, którzy wjechali na terytorium RP bez opieki osób sprawujących faktyczną pieczę nad nimi lub małoletnich obywateli Ukrainy, którzy wjechali na terytorium RP i bezpośrednio przed przybyciem byli umieszczeni w pieczy zastępczej na terytorium Ukrainy. Prowadzenie ewidencji w systemie informatycznym ma na celu ilościowe i jakościowe monitorowanie sposobu udzielonej opieki oraz miejsca i czasu udzielonej opieki, a także ma przeciwdziałać przestępstwom handlu ludźmi[4].

W tym kontekście wypada podkreślić, że informacje o dzieciach mogą mieć charakter danych osobowych i to w pewnym sensie szczególnie chronionych – w motywie 38 i 58 preambuły do RODO wskazuje się, że dzieci zasługują na szczególną ochronę, ponieważ mogą być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Co ciekawe, jeżeli dziecko urodzi się żywe, wówczas wszelkie informacje odnoszące się do niego i zebrane w trakcie życia płodowego powinny zostać uznane za dane osobowe tego dziecka[5].

Skoro informacja może mieć charakter danych osobowych wtedy, gdy dotyczy osoby fizycznej, **informacje o osobach prawnych nie mogą zostać uznane za dane osobowe**. Informacje rodzaju „ABC sp. z o.o.", czy XZY S.A." nie są więc danymi osobowymi tych podmiotów. Danymi osobowymi mogą być natomiast informacje o osobach fizycznych pełniących funkcje w organach osób prawnych – np. o członkach zarządu spółki czy fun-

[2] *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, s. 106.

[3] Zob. https://www.gov.pl/web/rodzina/mama-4-plus-rodzicielskie-swiadczenie-uzupelniajace (dostęp: 4.10.2022 r.).

[4] Zob. https://www.gov.pl/web/handel-ludzmi/rejestr-ukrainskich-dzieci-bez-opieki (dostęp: 4.10.2022 r.).

[5] *P. Barta*, *M. Kawecki*, *P. Litwiński*, (w:) Ogólne rozporządzenie..., s. 83.

dacji. Czasem może być też tak, że informacja o osobie prawnej będzie miała charakter danych osobowych, ale osoby fizycznej, która pełni np. rolę jej prezesa zarządu – o ile oczywiście identyfikuje go w sposób dostateczny.

Podobnie jest w przypadku organów władzy publicznej – informacja o organie jako takim nie ma charakteru danych osobowych tego organu, ale może mieć charakter danych osobowych jego piastuna.

Przykład

Informacja „burmistrz gminy X" z dużym prawdopodobieństwem stanowi informację o charakterze danych osobowych osoby piastującej ten urząd, ale nie stanowi danych osobowych organu wykonawczego gminy, jakim jest burmistrz.

Ogólne rozporządzenie o ochronie danych znajduje w całości zastosowanie do przetwarzania danych osobowych dotyczących osób fizycznych prowadzących działalność gospodarczą, ponieważ tego rodzaju informacje mogą mieć – na zasadach ogólnych – charakter danych osobowych. Na gruncie RODO nie istnieją więc żadne podstawy do wyodrębniania danych osobowych osób fizycznych prowadzących działalność gospodarczą spośród ogółu danych osobowych objętych jego zastosowaniem.

Ważne

Informacje o osobach fizycznych prowadzących działalność gospodarczą mogą stanowić, na ogólnych zasadach, informacje o charakterze danych osobowych.

Informacja dotycząca osoby fizycznej ma charakter danych osobowych wtedy, gdy ta osoba jest osobą zidentyfikowaną lub możliwą do zidentyfikowania.

Ogólne rozporządzenie o ochronie danych nie definiuje pojęcia osoby zidentyfikowanej, lecz jedynie pojęcie osoby możliwej do zidentyfikowania. Rozróżnienie pomiędzy tymi pojęciami powinno zostać oparte na definicji osoby możliwej do zidentyfikowania – skoro osobą możliwą do zidentyfikowania jest osoba, którą można bezpośrednio lub pośrednio zidentyfikować, za osobę zidentyfikowaną należy uznać taką osobę, której tożsamość jest znana administratorowi danych. Administrator danych powinien więc mieć obiektywną możliwość powiązania konkretnej informacji z konkretną osobą, bez konieczności podejmowania jakichkolwiek innych działań, składających się na proces ustalania tożsamości[6].

Identyfikacja osoby nie wymaga znajomości jej imienia lub nazwiska, wymaga natomiast znajomości pewnych unikalnych cech tej osoby, które odróżniają ją od innych osób. Jeden z autorów w czasach przedpandemicznych nałogowo ilustrował to następującym przykładem: prowadząc zajęcia ze studentami, wybierał jedną osobę ubraną w charakterystyczny sposób i mówił np. tak: „osoba w czerwonej marynarce". Ponieważ na sali była jedna tak ubrana osoba, była ona osobą zidentyfikowaną, bez żadnej wiedzy na temat jej imienia, nazwiska, czy innych cech. Analogicznie, wypowiedź typu: prezydent wskazanego miasta, pozwala na jednoznaczną identyfikację osoby sprawującej tę funkcję – status danych osobowych zależy często od kontekstu, w jakim informacje te występują. Z ko-

[6] *P. Barta*, *M. Kawecki*, *P. Litwiński*, (w:) Ogólne rozporządzenie..., s. 86.

lei czasem nawet znajomość imienia i nazwiska nie będzie pozwalała na jednoznaczną identyfikację osoby, np. w przypadku bardzo popularnych nazwisk, gdyż osób noszących takie samo imię i nazwisko może być wiele[7].

Z kolei osoba możliwa do zidentyfikowania to osoba, której tożsamości nie znamy, ale którą to tożsamość możemy ustalić. Ale skąd mamy wiedzieć, czy możemy ustalić tożsamość konkretnej osoby? W odpowiedzi na to pytanie pomaga nam motyw 26 preambuły do RODO, zgodnie z którym: by 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 przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany 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.

„Rozsądnie prawdopodobne", „uzasadnione prawdopodobieństwo", „obiektywne czynniki"– czyli w praktyce co?

Po pierwsze, nie interesuje nas to, jakie działania podjęto w celu identyfikacji – interesuje nas możliwość, a więc działania takie, które są potencjalnie dostępne dla tego, kto tej identyfikacji ma dokonać. Po drugie, identyfikacja osoby fizycznej może nastąpić zasadniczo na dwa sposoby:

1) bezpośrednio – np. przez imię i nazwisko, NIP, PESEL, numer identyfikacyjny pracownika, numer umowy przypisany do konkretnej osoby;
2) pośrednio – np. przez identyfikatory internetowe w postaci adresu IP czy też identyfikatora plików *cookies* lub za pomocą szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Nie można też zapominać, że identyfikacja osoby fizycznej może mieć miejsce również w oparciu o czynniki określające cechy takie, jak np.:

1) fizyczne (np. budowa ciała, fryzura, sposób chodzenia);
2) fizjologiczne (np. wyniki spirometrii, EKG, pomiar ciśnienia tętniczego);
3) umysłowe;
4) ekonomiczne (np. wynagrodzenie otrzymywane na danym stanowisku w miejscu pracy, najbogatszy człowiek w Polsce);
5) kulturowe (np. język, system wartości i przekonań, tradycje, rytuały, zwyczaje lub zachowania danej społeczności)[8];
6) społeczne (np. przynależność do grup/zbiorów społecznych, do regionu, kategorii zawodowej, wieku).

Po trzecie, oceniając, czy konkretny podmiot może zidentyfikować konkretną osobę, uwzględniamy nie tylko informacje, jakie ten podmiot ma we własnych zasobach, ale

[7] *P. Fajgielski*, Ogólne rozporządzenie..., s. 110.

[8] Zob. https://znaczenia.com.pl/znaczenie-tozsamosc-kulturowa-co-to-jest-pojecie-i-definicja-znaczenia/ (dostęp: 4.10.2022 r.).

także takie, do których może mieć dostęp. Znając więc np. numer NIP przedsiębiorcy, powinniśmy uwzględniać to, że stosunkowo łatwo można przy pomocy tego numeru odnaleźć przedsiębiorcę w CEIDG, a więc dokonać jego pełnej identyfikacji.

Po czwarte wreszcie, spełnienie przesłanki identyfikacyjnej weryfikowane powinno być poprzez zakres aktywności administratora lub innej osoby o określonym rozsądnym prawdopodobieństwie, ograniczonym jednak przez zobiektywizowane czynniki, jak: koszt i czas potrzebne do jej zidentyfikowania, technologię dostępną w momencie przetwarzania danych czy postęp technologiczny[9].

Przykład

Ta sama informacja dla jednego podmiotu może mieć charakter danych osobowych, dla innego natomiast nie: np. numer rachunku bankowego ma charakter danych osobowych dla banku, który ten rachunek prowadzi i np. dla pracodawcy, który na ten rachunek przekazuje wynagrodzenie pracownika, ale dla osoby postronnej już takiego charakteru nie ma, bo osoba ta nie jest w stanie ustalić, kto jest posiadaczem tego rachunku.

Zakres czynności, które administrator danych musi podjąć w celu identyfikacji osoby fizycznej, można określić jako próg identyfikowalności: jeżeli przekroczenie tego progu wymaga ogromnych kosztów czy poświęcenia długiego czasu, to choć informacja potencjalnie umożliwia identyfikację, nie powinna zostać uznana za mającą charakter danych osobowych. W tym kontekście warto podkreślić, że ten próg identyfikowalności spada wraz z upływem czasu. Jeszcze kilkanaście lat temu adres poczty elektronicznej w rodzaju misiu@cośtam.pl nie umożliwiał identyfikacji jego posiadacza. Obecnie natomiast wystarczy skorzystać z najpopularniejszej na świecie wyszukiwarki internetowej i jeżeli Misiu gdziekolwiek – w szczególności w mediach społecznościowych – tego adresu użył, wyszukiwarka nas do tego Misia odeśle. Ten próg identyfikowalności jest też relatywnie niżej usytuowany w przypadku podmiotów publicznych – ponieważ, co do zasady, dysponują one szerszym dostępem do rejestrów publicznych, niż podmioty z sektora prywatnego.

Podsumowując, abyśmy mogli mówić o danych osobowych, powinniśmy przeanalizować, czy mamy do czynienia z:

informacją lub informacjami	nie jest konieczne, by informacja ta umożliwiała sama w sobie zidentyfikowanie osoby, której dane dotyczą, istotne jest jednak, że jej charakter powinien być oceniany indywidualnie dla każdego podmiotu, który dysponuje informacjami
dotyczącymi zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,	oceniając, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może, racjonalnie rzecz biorąc, posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby
którą możemy zidentyfikować bezpośrednio	po imieniu i nazwisku, adresie e-mail, pseudonimie, tatuażu, sposobie wysławiania się, sposobie poruszania się, stylu ubierania się, charakterze pisma, tembrze głosu

[9] *D. Lubasz*, *A. Szkurłat*, Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych, MoP 2021, Nr 23 – dodatek, s. 79.

lub pośrednio	na podstawie np. adresu IP, danych o lokalizacji czy identyfikatora plików *cookies* lub za pomocą szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

A czy można w stosunku do jakiejkolwiek kategorii informacji z pewnością powiedzieć, że ma ona charakter danych osobowych? Nie, nie można – nawet numer Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL), nadawany na podstawie art. 15 i n. EwidLU, mimo tego, że jednoznacznie identyfikuje osobę fizyczną, to jednak nie działa w ten sposób, że każdy zainteresowany może sprawdzić dowolny numer PESEL. Udostępnianie danych ze zbioru PESEL na rzecz osób i jednostek organizacyjnych innych niż organy administracji publicznej oraz podmioty realizujące zadania publiczne wymaga wykazania przez wnioskodawców interesu prawnego lub w pewnych wypadkach interesu faktycznego i zgody osoby, której dotyczą udostępniane informacje. W powszechnym ujęciu numer ewidencyjny PESEL nie będzie miał zawsze charakteru danych osobowych – ale w stosunku do organów administracji publicznej już tak, co może służyć za kolejną ilustrację tezy o tym, że próg identyfikowalności osób fizycznych jest odpowiednio niżej usytuowany w przypadku podmiotów publicznych.

Z największą dozą pewności można przypisać osobowy charakter pewnym zestawom informacji, takim jak imię, nazwisko i adres zamieszkania czy np. imię, nazwisko i numer telefonu. Samodzielnie występująca informacja o numerze telefonu, co do zasady, nie będzie miała charakteru danych osobowych, ponieważ w tej postaci umożliwia wyłącznie kontakt z osobą użytkownika, a nie zaś jej identyfikację.

Przykład

Adres poczty elektronicznej może mieć samodzielnie charakter danych osobowych, o ile sam umożliwia identyfikację osoby, której dotyczy – będzie tak typowo w przypadku służbowych adresów poczty elektronicznej, które zazwyczaj zawierają nazwisko lub imię i nazwisko oraz informację o miejscu pracy. Fantazyjne adresy poczty elektronicznej, jak choćby przywołany już „misiu", takiej identyfikacji nie umożliwiają. Z drugiej strony, jeżeli dostawca usługi poczty elektronicznej świadczonej na rzecz Misia dysponuje informacjami umożliwiającymi identyfikację tej osoby, np. jej imieniem, nazwiskiem i adresem zamieszkania, wówczas dla tego podmiotu adres poczty elektronicznej misiu@cośtam.pl w sposób oczywisty będzie miał charakter danych osobowych. Podobnie, jeżeli Misiu posłuży się swoim adresem np. w sklepie internetowym, podając też swoje imię, nazwisko i adres do doręczeń: wówczas dla podmiotu prowadzącego ten sklep, adres misiu@cośtam.pl będzie miał charakter danych osobowych.

2. Dane osobowe w orzecznictwie sądowym

Wbrew temu, co można by przypuszczać, nie doczekaliśmy się wielu wyroków sądowych – tak na poziomie europejskim, jak i krajowym – dotyczących samego pojęcia danych osobowych. W przypadku orzecznictwa TS UE (wcześniej ETS), trzeba wymienić:

1) wyrok w sprawie *Bodil Lindqvist*, w którym ETS uznał, że termin „dane osobowe" użyty w art. 3 ust. 1 dyrektywy 95/46/WE [obecnie nieobowiązująca – przyp. aut.] obejmuje m.in. nazwisko osoby w połączeniu z jej numerem telefonu lub informa-

cjami dotyczącymi jej warunków pracy czy sposobów spędzania przez nią wolnego czasu (wyr. TS z 6.11.2003 r., C-101/01, Legalis);
2) wyrok w sprawie *Promusicae*, w którym TS UE przyjął, że nazwiska i adresy osób fizycznych stanowią ich dane osobowe w rozumieniu art. 2 pkt a dyrektywy 95/46/WE [obecnie nieobowiązującej – przyp. aut.] (wyr. TS z 29.1.2008 r., C-275/06, Legalis);
3) wyrok w sprawie *Scarlet*, w którym TS UE stanął na stanowisku, że adresy IP użytkowników korzystających z sieci Internet mają dla dostawcy usługi dostępu do Internetu charakter danych osobowych, ponieważ pozwalają na precyzyjną identyfikację tych użytkowników (wyr. TS z 24.11.2011 r., C-70/10, Legalis);
4) wyrok w sprawie *Peter Nowak*, w którym TS UE uznał, że treść odpowiedzi udzielonych w teście egzaminacyjnym oraz komentarze naniesione przez egzaminatora dotyczące tych odpowiedzi należy uznać za dane osobowe (wyr. TS z 20.12.2017 r., C-434/16, Legalis);
5) wyrok w sprawie *Patrick Breyer*, w którym TS UE uznał, że dynamiczny adres IP ma charakter danych osobowych dla niemieckiego podmiotu prowadzącego stronę internetową, w logach której ten adres został zapisany (wyr. TS z 19.10.2016 r., C-582/14, Legalis).

Pierwsze trzy orzeczenia wydają się raczej oczywiste i nie budzą specjalnych wątpliwości, zwłaszcza z perspektywy czasu. Z kolei wyrok w sprawie *Peter Nowak* (C-434/16) oparty został na założeniu, że danymi osobowymi może być każda informacja odnosząca się do osoby fizycznej – w tym przejaw jej twórczości oraz to, co na jej temat zapisały inne osoby. Wychodząc z tego założenia, TS UE wskazał, że treść odpowiedzi udzielonych w teście egzaminacyjnym należy uznać za dane osobowe ze względu na fakt, że odzwierciedlają one „poziom wiedzy i umiejętności osoby przystępującej do egzaminu w danej dziedzinie i, w odpowiednim przypadku, sposób jej rozumowania, wnioskowania i przyjęte przez nią krytyczne podejście. W przypadku egzaminu pisanego odręcznie odpowiedzi te zawierają poza tym informacje odnoszące się do charakteru pisma". Z kolei treść komentarzy egzaminatorów „odzwierciedla (...) wyrażoną przez egzaminatora opinię czy ocenę indywidualnych osiągnięć danej osoby na tym egzaminie, a w szczególności poziomu jej wiedzy i umiejętności w danej dziedzinie. Komentarze te mają zresztą na celu właśnie udokumentowanie dokonanej przez egzaminatora oceny wyników osiągniętych przez osobę przystępującą do egzaminu (...)". Na tej samej zasadzie za informacje o charakterze danych osobowych trzeba uznać np. notatki z przebiegu rozmowy rekrutacyjnej czy oceny z testu stanowiącego element procesu rekrutacji.

Orzeczenie zapadłe w sprawie *Patrick Breyer* (C-582/14) przyczyniło się do powstania wielu nieścisłości i zwyczajnego szumu informacyjnego w kontekście pojęcia danych osobowych. W tym przypadku TS UE stanął przed koniecznością odpowiedzi na pytanie, czy administrator, który przetwarza adres IP, ale nie dysponuje na co dzień narzędziem do identyfikacji osoby korzystającej z tego adresu, ale takim narzędziem dysponuje strona trzecia, ma do czynienia z danymi osobowymi.

Odpowiadając na to pytanie TS UE wskazał, że aby uznać informację za mającą charakter danych osobowych nie jest konieczne, by informacja ta umożliwiała sama w sobie zidentyfikowanie osoby, której dane dotyczą (identyfikacja pośrednia). W motywie 26 dyrek-

tywy 95/46/WE wskazano bowiem, że w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może, racjonalnie rzecz biorąc, posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby. Aby informacje mogły zostać uznane za dane osobowe, nie jest także wymagane, by wszystkie informacje umożliwiające identyfikację osoby, której dane dotyczą, musiały znajdować się w rękach tylko jednej osoby.

W opinii TS UE dla oceny charakteru prawnego informacji istotne jest więc zweryfikowanie, czy połączenie danych osobowych, którymi dysponuje podmiot, z danymi osobowymi, w których posiadaniu jest strona trzecia, stanowi sposób, który racjonalnie rzecz biorąc, może zostać zastosowany w celu zidentyfikowania osoby, której dane dotyczą. W praktyce oznacza to, że identyfikacja osoby fizycznej mogłaby być niemożliwa, gdyby była:

1) zakazana prawem lub
2) 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.

Mimo że wyrok w sprawie *Patrick Breyer* zapadł na gruncie nieobowiązującej już dyrektywy 95/46/WE, wiele wskazuje na to, iż zachowuje on aktualność na gruncie przepisów RODO. Co więcej, przepisy RODO zdają się dodatkowo akcentować sytuację tego podmiotu, który miałby dokonać identyfikacji – przy ocenie charakteru prawnego informacji trzeba jeszcze bowiem uwzględnić wymóg, aby istniało „uzasadnione prawdopodobieństwo", że dany środek identyfikacji zostanie wykorzystany. Nie każdy więc przypadek, w którym dany środek identyfikacji jest potencjalnie dostępny, będzie oznaczał, że środek ten zostanie wykorzystany. Oznacza to, że na gruncie przepisów RODO charakter prawny informacji powinniśmy oceniać według tzw. podejścia subiektywnego, a więc badać, „czy podmiot mający dostęp do danych (będących w posiadaniu osoby trzeciej) ma możliwość posłużenia się nimi w ramach własnych środków w celu identyfikacji danej osoby", nie zaś według tzw. podejścia obiektywnego, które zakłada, że możliwość identyfikacji osoby trzeba rozpatrywać niezależnie od możliwości podmiotu, który tej identyfikacji ma dokonywać – informacja ma charakter danych osobowych, jeżeli „do dokonania identyfikacji wystarczy połączenie z danymi dostarczonymi przez osobę trzecią"[10]. Będzie tak dlatego, że definicja danych osobowych, wynikająca z art. 4 pkt 1 RODO, zawiera nowy element, nieznany dyrektywie – element uzasadnionego prawdopodobieństwa – który przesądza o konieczności stosowania subiektywnego podejścia do przesłanki identyfikowalności osoby fizycznej[11].

Ciekawy problem związany z pojęciem danych osobowych dotyczy kwalifikacji prawnej numeru rejestracyjnego pojazdu. Pogląd zakładający, że numer rejestracyjny pojazdu może prowadzić do identyfikacji osoby, a zatem stanowi on dane osobowe, został wyra-

[10] Zob. opinia Rzecznika Generalnego *M. Camposa Sáncheza-Bordony*, przedstawiona do sprawy *Breyer*, https://curia.europa.eu/juris/document/document.jsf?text=&docid=178241&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=311064 (dostęp: 24.10.2022 r.); zob. także *P. Litwiński*, Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku TS z 19.10.2016 r. w sprawie C-582/14 Patrick Breyer, EPS 2017, Nr 5.

[11] *P. Barta*, *M. Kawecki*, *P. Litwiński*, (w:) Ogólne rozporządzenie..., s. 91.

żony przez WSA w Warszawie w wyroku z 13.4.2017 r. (VII SA/Wa 1069/16, Legalis). Z kolei WSA w Krakowie w wyroku z 14.12.2016 r. (II SA/Kr 1339/16, Legalis) zajął stanowisko przeciwne, uznając, że ewentualne powiązanie numeru rejestracyjnego z osobą fizyczną wymagałoby nadzwyczajnych nakładów i nie jest czynnością łatwą, a sam numer rejestracyjny pojazdu służy przede wszystkim identyfikacji pojazdu i do niego jest przypisany, nie jest natomiast możliwe, w sposób prosty i łatwy, powiązać numer rejestracyjny pojazdu z osobą właściciela lub posiadacza pojazdu. Ciekawy pogląd wyraził w tym kontekście WSA w Gliwicach w wyroku z 31.10.2018 r. (II SA/Gl 593/18, Legalis), uznając, że tradycyjny numer rejestracyjny, składający się z liter i cyfr, nie jest daną osobową, gdyż określenie tożsamości osoby fizycznej wymagałoby nadmiernych kosztów, czasu lub działań. Jednocześnie jednak sąd zauważył, że istnieje możliwość oznaczenia pojazdu tzw. tablicami rejestracyjnymi indywidualnymi, na których litera i cyfra stanowią wyróżnik województwa, zaś kolejne litery w liczbie od 3 do 5 stanowią wyróżnik indywidualny pojazdu, w którym nie więcej niż dwie ostatnie litery można zastąpić liczbą i nie ma żadnych przeszkód, by takie indywidualne oznaczenie w sposób dość łatwy lub wręcz wprost pozwalało zidentyfikować właściciela pojazdu, jeśli będzie to określenie dla niego bardzo charakterystyczne i zindywidualizowane, pozwalające się zorientować o jaką osobę chodzi.

Naczelny Sąd Administracyjny w wyroku z 28.6.2019 r. (I OSK 2063/17, Legalis) uznał, że numery rejestracyjne pojazdów nie mają charakteru danych osobowych, ponieważ brak jest możliwości powiązania ich bez nadmiernego wysiłku i kosztów, z osobami fizycznymi, „które dają się zidentyfikować". Takie stanowisko sądu zostało ocenione krytycznie z uwagi na to, że wyrok sądu zapadł w kontekście przetwarzania danych osobowych przez m.st. Warszawa, które ma dostęp do danych przetwarzanych w CEPiK[12]. Tym samym, jak się wydaje, m.st. Warszawa miało – i nadal ma – możliwość identyfikacji osób fizycznych na podstawie numerów rejestracyjnych pojazdów.

Obecnie jesteśmy świadkami toczącej się dyskusji, czy pliki *cookies* lub adres IP są zawsze danymi osobowymi. Zgodnie z motywem 30 RODO 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. Z motywu tego nie wynika jednak, że adres IP lub plik *cookie* zawsze mają charakter danych osobowych – takie podejście, przynajmniej w orzecznictwie sądowym, zdaje się dominować w polskich realiach. Przywołać tu można w szczególności wyrok WSA w Warszawie z 11.7.2022 r. (II Sa/Wa 3993/21, Legalis), w którym wskazano, że nie ma podstaw, by uznać, że adres IP – niezależnie od tego, czy jest adresem statycznym, czy dynamicznym oraz niezależnie od tego, kto jest dysponentem i jakie istnieją możliwości wykorzystania go w celu identyfikacji osoby fizycznej, należy zawsze traktować jako daną osobową. Takie stanowisko sądu obecne jest w orzecznictwie co najmniej od 2011 r., kiedy to NSA (OSK 1079/10, Legalis) uznał, że tylko tam, gdzie numer IP pozwala pośrednio na identyfikację konkretnej osoby fizycznej, powinien on być uznany za dane osobowe.

[12] *P. Barta, M. Kawecki, P. Litwiński*, (w:) Ogólne rozporządzenie..., s. 92.

Tymczasem w opinii Grupy Roboczej Art. 29 (opinia 4/2007) w sprawie pojęcia danych osobowych, przyjętej 20.6.2007 r.[13], stwierdzono, że: „może (...) zdarzyć się tak, że osoba zbierająca takie dane co prawda nie ma lub co do zasady nie jest w stanie «w normalnym trybie» uzyskać innych informacji pozwalających na identyfikację, jednak zbiera takie informacje właśnie w celu ewentualnej późniejszej identyfikacji". Mamy więc do czynienia z uznaniem informacji za stanowiącą dane osobowe niejako na zapas. Grupa Robocza Art. 29 rozszerzyła jeszcze rozumienie pojęcia danych osobowych w opinii 1/2008 z 4.4.2008 r.[14], dotyczącej kwestii ochrony danych w związku z wyszukiwarkami. W opinii tej Grupa Robocza Art. 29 przyjęła w odniesieniu do adresów IP, że mimo iż zwykle nie umożliwiają one zidentyfikowania użytkownika przez samą wyszukiwarkę, to – co do zasady – dane niezbędne do identyfikacji użytkownika adresu IP są osiągalne dla operatora wyszukiwarki. Z tego względu Grupa Robocza Art. 29 przyjęła, że dopóki operator wyszukiwarki nie jest w stanie potwierdzić z absolutną pewnością (*with absolute certainty*), że dane te są powiązane z użytkownikiem, który nie może zostać zidentyfikowany, musi traktować wszystkie adresy IP jak dane osobowe. Grupa Robocza Art. 29 uznała, że nawet usunięcie ostatnich 3 cyfr adresu nie może przesądzać o jego anonimizacji, gdyż pozostawia to 254 potencjalne adresy IP, które mogą bez wielkich komplikacji zostać odtworzone.

Stanowisko Grupy Roboczej Art. 29 zdaje się akceptować Prezes UODO – w szeroko opisywanej w mediach decyzji skierowanej do firmy iSecure sp. z o.o.[15] organ uznał, że zarówno adres IP, jak również ID plików *cookies*, z uwagi na uzasadnione prawdopodobieństwo zidentyfikowania osoby fizycznej, stanowią dane osobowe. Decyzja ta została jednak uchylona przez WSA w Warszawie w przywołanym już wyżej wyroku z 11.7.2022 r. (II Sa/Wa 3993/21, Legalis).

Innym przykładem sporu o to, czy informacja ma charakter danych osobowych, czy też nie, jest problem udostępniania przez Głównego Geodetę Kraju numerów ksiąg wieczystych za pośrednictwem Geoportalu. W ocenie Prezesa UODO, numery ksiąg wieczystych mają charakter danych osobowych, co zostało wyrażone m.in. w decyzji z 24.8.2020 r. (DKN.5112.13.2020, Legalis) i potwierdzone w wyroku WSA w Warszawie z 5.5.2021 r. (I SA/Wa 2222/20, Legalis): sąd uznał, że podane do publicznej wiadomości na portalu GEOPORTAL numery ksiąg wieczystych pozwalają na identyfikację osób, których dane zawarte są w księdze wieczystej. Tymczasem Główny Geodeta Kraju konsekwentnie prezentuje stanowisko, zgodnie z którym numery ksiąg wieczystych nie mają charakteru danych osobowych i na ostateczne rozstrzygnięcie tej kwestii zapewne przyjdzie nam poczekać na wyrok NSA.

13 WP 136, www.giodo.gov.pl.
14 WP 148, www.giodo.gov.pl.
15 Zob. *M. Lothamer*, Ciasteczka nie zawsze smakują najlepiej, https://www.isecure.pl/blog/ciasteczka-nie-zawsze-smakuja-najlepiej/ (dostęp: 4.10.2022 r.).

3. Kategorie danych osobowych

W przepisach RODO wyróżnione zostały dwie kategorie danych osobowych:

1) tzw. **dane zwykłe** – chociaż nie zostały one w taki sposób określone w RODO, przyjmujemy, że są to wszystkie dane, które nie są danymi szczególnej kategorii;
2) **dane szczególnych kategorii** – wymienione w art. 9 RODO. Dotyczą one obszarów prywatnych wręcz intymnych, takich jak:
   a) pochodzenie rasowe lub etniczne,
   b) poglądy polityczne,
   c) przekonania religijne lub światopoglądowe,
   d) przynależność do związków zawodowych,
   e) dane genetyczne lub biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
   f) dane dotyczące zdrowia,
   g) dane dotyczące seksualności lub orientacji seksualnej osoby.

Katalog danych szczególnej kategorii jest katalogiem zamkniętym. Oznacza to, że dane nie mieszczące się w tym katalogu trzeba zakwalifikować do tzw. danych zwykłych. Warto przy tym pamiętać, że dane osobowe należące do kategorii danych zwykłych, które pośrednio mogą prowadzić do ujawnienia informacji mających charakter danych osobowych szczególnych kategorii, należy traktować jako dane zaliczające się do tej drugiej grupy (zob. wyr. TS UE z 1.8.2022 r. w sprawie *Vyriausioji tarnybinės etikos komisija*, C-184/20, Legalis; w realiach sprawy ujawnienie danych osobowych partnera w zw. z przepisami antykorupcyjnymi uznano za umożliwiające wnioskowanie o kwestiach życia seksualnego).

4. Pseudonimizacja danych osobowych

Wejście w życie RODO zmieniło w znacznym stopniu świat IT, a tym samym systemy informatyczne stanęły przed nowymi wyzwaniami. Odpowiednie przechowywanie, przetwarzanie i zapewnienie tym samym prywatności danych osobowych stało się jedną z głównych zasad w branży technologicznej. Często, kiedy poruszane jest zagadnienie dotyczące przetwarzania danych osobowych, pojawia się też nierozłącznie aspekt dotyczący pseudonimizacji i anonimizacji danych osobowych. Te pojęcia, mimo iż nierozerwalnie związane są z ochroną danych osobowych, to znacznie się od siebie różnią.

Czym jest pseudonimizacja? Definicję tego pojęcia znajdziemy w art. 4 ust. 5 RODO, a brzmi ono następująco:

„pseudonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej".

W podobny sposób pseudonimizację opisuje ENISA, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa – pseudonimizacja polega na przekształceniu danych osobowych w ten sposób, aby niemożliwe było zidentyfikowanie, do kogo te dane należą, bez dodatkowych informacji, które to informacje powinny być przechowywane oddzielnie od informacji spseudonimizowanej[16]. Pseudonimizacja, w przeciwieństwie do anonimizacji, jest procesem odwracalnym. Zatem pseudonimizacja zapewnia anonimowość użytkownikowi, utrzymując przy tym korelację różnych danych w całości.

Podstawowym założeniem, jakie powinno przyświecać tworzeniu aplikacji bądź systemu, jest to, że całość powinna odbywać się zgodnie z zasadami „ *Privacy by Design*" (uwzględnienie ochrony danych już w fazie projektowania) oraz „*Privacy by Default*" (czyli zasady prywatności w ustawieniach domyślnych). O prywatności, jak i o bezpieczeństwie danych osobowych należy pamiętać już na etapie wyboru rozwiązań technologicznych. Tworząc aplikację bądź system, w którym będą przetwarzane dane osobowe, na samym początku tworzenia musimy wiedzieć, jakie konkretnie dane będzie przetwarzała dana aplikacja oraz w jaki sposób zapewnimy właśnie jeden z podstawowych wymogów, jakim jest pseudonimizacja i anonimizacja danych osobowych.

Wspomniana wyżej zasada znalazła odzwierciedlenie w art. 25 ust. 1 RODO, zgodnie z którym, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja i anonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą. Dlatego też pseudonimizacja wymieniana jest jako jeden z elementów zabezpieczeń, które administrator danych osobowych powinien wziąć pod uwagę.

Typowe sposoby pseudomizacji danych osobowych to:

1) szyfrowanie z zastrzeżeniem, że klucz (algorytm) dekodujący przechowywany jest w innej bazie;
2) zastępowanie części danych ciągiem znaków;
3) zaciemnianie lub maskowanie liter;
4) modyfikacja danych w taki sposób, aby pokazywały przybliżone wartości.

Jednym z istotnych elementów, w którym powinniśmy stosować zasadę pseudonimizacji, są logi systemowe. Cechą wszystkich systemów informatycznych i aplikacji jest to, że zapisują logi, czyli prowadzą dzienniki swoich działań. Bez logów niemożliwe byłoby zarówno bieżące nadzorowanie takich systemów, jak i dochodzenie przyczyn ich awarii bądź też wskazanie zmian, jakie zostały dokonane. Co do zasady, logi systemowe powinny być przechowywane w innym miejscu niż główna baza danych. Często właśnie to w logach systemowych możemy znaleźć dużą liczbę danych osobowych, a stosując od-

[16] Pseudonymisation techniques and best practices Recommendations on shaping technology according to data protection and privacy provisions, ENISA 2019, s. 9.

powiednią metodę pseudonimizacji, możemy wyeliminować przetwarzanie danych osobowych w logach systemowych, a tym samym podnieść poziom bezpieczeństwa danych osobowych.

Przykład

Przykład pseudonimizacji:

Dane osobowe:

Login	jan_kowalski
Imię i Nazwisko	Jan Kowalski
e-mail	Jan_kowalski@twojafirma.pl

Pseudonimizacja danych osobowych:

Login	1@345890#$!
Imię i Nazwisko	456@5642%&
e-mail	693%@874%#

Jak widać na przykładzie powyżej, dane osobowe zostały zastąpione ciągiem znaków, tym samym inny system po wprowadzeniu w odpowiednie miejsce ciągu znaków powinien całość odkodować.

5. Anonimizacja danych osobowych

W przepisach RODO nie znajdziemy definicji procesu anonimizacji danych osobowych, choć w polskim systemie prawnym można odnaleźć legalną definicję anonimizacji danych[17]. W ślad za opinią Grupy Roboczej Art. 29 (opinia 05/2014 on Anonymisation Techniques)[18] przyjmuje się, że anonimizacja oznacza takie przetworzenie danych osobowych, w efekcie którego powstałe informacje nie mogą zostać wykorzystane w celu zidentyfikowania osoby fizycznej ani przez administratora dokonującego anonimizacji, ani przez jakikolwiek inny podmiot[19]. W ten sposób informacje, które przed anonimizacją były danymi osobowymi, przestają nimi być. Istotny jest fakt, że tego działania nie można cofnąć, jest ono trwałe i nieodwracalne. Możliwe jest pozostawienie jedynie danych statystycznych, np. na potrzeby analiz czy raportów.

17 Zgodnie z art. 3 pkt 1 ustawy z 16.9.2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. Nr 230, poz. 1371), anonimizacja to przekształcenie danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej albo jeżeli przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań.

18 Zob. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (dostęp: 4.10.2022 r.).

19 Opinia Grupy Roboczej Art. 29, 05/2014 on Anonymisation Techniques, s. 5.

Stosowanie anonimizacji danych osobowych może przynieść wymierne korzyści – można wśród nich wymienić możliwość:

1) wykorzystania danych zanonimizowanych do innych celów, bo nie stanowią one już danych osobowych;
2) przechowywania takich danych przez nieograniczony czas.

Anonimizację powinno się stosować w momencie ustania podstawy prawnej do dalszego przetwarzania danych osobowych lub po upłynięciu okresu retencji danych. Dlatego warto na samym początku podczas tworzenia danego systemu bądź też procesu, w ramach którego będą przetwarzane dane osobowe, doprecyzować, że dane osobowe są usuwane po z góry ustalonym czasie, a całość poprzedzona jest wcześniejszym konkretnym komunikatem, że zbliża się czas anonimizacji danych.

Ważne

Jeżeli anonimizacja następuje w systemach informatycznych, należy w wewnętrznych procedurach ustalić zasady cyklicznej weryfikacji, czy dane zostały prawidłowo zanonimizowane.

Podstawa prawna:

- art. 4 pkt 1 RODO.

Paweł Litwiński

Rozdział II. Przetwarzanie danych osobowych w sektorze publicznym – administrator i przetwarzający

1. Uwagi ogólne

Prawidłowa kwalifikacja podmiotów biorących udział w procesach przetwarzania danych osobowych to kwestia fundamentalna z perspektywy zapewnienia zgodności takiego przetwarzania z prawem. Dlaczego? Z dwóch powodów. Po pierwsze, **inaczej kształtują się obowiązki administratora danych, a inaczej przetwarzającego**. Po drugie, co stanowi konsekwencję poprzedniego, **inny jest zakres odpowiedzialności tych podmiotów**. W konsekwencji, błąd popełniony przy określaniu roli podmiotów przetwarzających dane osobowe przekłada się na cały proces przetwarzania danych osobowych, a jego konsekwencje mogą być bardzo daleko idące.

W każdym procesie przetwarzania danych osobowych mogą występować dwie kategorie podmiotów:

1) **administrator danych osobowych** – podmiot, który ustala cele i sposoby przetwarzania danych osobowych;
2) **podmiot przetwarzający**, który przetwarza dane osobowe w imieniu administratora danych.

To, czy określony podmiot pełni rolę administratora, czy przetwarzającego, wynika wyłącznie ze stanu faktycznego – albo ustala cele i sposoby i wtedy jest administratorem, albo przetwarza w imieniu administratora i wtedy jest podmiotem przetwarzającym.

Ważne

Statusu w procesie przetwarzania danych osobowych nie można wybrać, nie można określić umownie czy w inny sposób między zaangażowanymi podmiotami. Ten status zawsze wynika z okolicz-