Mateusz Niedźwiecki
(Uniwersytet Wrocławski)

Pseudonimizacja jako nowy środek zabezpieczenia danych osobowych w świetle zmian prawnych w UE – wybrane aspekty

Abstract

Pseudonymization as a new means of securing personal data in the light of EU legal changes – selected aspects

The article is about question of pseudonymization which is a way of protecting personal data. It means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. This concept appears for the first time in the new EU regulation of 2016.

The article presents main changes related to new regulation, describes the process of pseudonymization as well as selected methods of its use. It also presentes disadvantages that may be associated with this technique. The author also refers to the practical aspect citing the results of a study commissioned by Dell in 2016 on the new regulation.

Keywords: pseudonymization, personal data protection, regulation, amendment, GDPR.

1. Wstęp

Od kilku lat w instytucjach Unii Europejskiej (dalej: UE) trwały intensywne prace nad reformą ochrony danych osobowych. Obowiązująca

obecnie dyrektywa 95/46/WE Parlamentu Europejskiego i Rady[1] harmonizująca cały sektor ochrony danych osobowych była opracowywana w połowie lat dziewięćdziesiątych co sprawia, iż przepisy te są niedostosowane do wielu ważnych zmian technologicznych i realiów XXI wieku[2]. Regulacje Dyrektywy nie uwzględniają obecnej skali i stopnia przetwarzania danych osobowych. Przykładowo warto nadmienić, że w 1995 roku uruchomiono po raz pierwszy platformę handlową Amazon, a w 1998 roku działać zaczęła wyszukiwarka internetowa Google. Co więcej, kraje członkowskie UE wdrażały ww. Dyrektywę w trakcie implementacji w odmienny sposób, niejako „po swojemu", co było przyczyną późniejszych zróżnicowań w sposobach urzeczywistniania ochrony danych osobowych w całej Unii[3]. Pośrednio skutkowało to również upowszechnieniem istniejącego poglądu w społeczeństwie, wedle którego z przetwarzaniem danych, zwłaszcza w zakresie działalności prowadzonej w Internecie łączą się uzasadnione ryzyka[4].

Rozwiązaniem powyższych problemów ma być Rozporządzenie[5], które zostało przyjęte w dniu 14 kwietnia 2016 roku przez Parlament Europejski, a od 25 maja 2018 roku podlegać będzie bezpośredniemu zastosowaniu na obszarze całej UE. Bez wątpienia nowe przepisy prawne w niektórych obszarach zakładają daleko idące zmiany i sporo nieznanych dotąd obowiązków, w związku z czym przewidziano dwuletni okres przejściowy. Podmioty zobowiązane do stosowania nowych przepisów mają więc czas na dostosowanie procedur do wymogów powyższego Rozporządzenia i zapoznanie się z nową regulacją.

Warto również podkreślić, iż europejski ustawodawca decydując się na reformę przepisów z zakresu ochrony danych osobowych poprzez akt

1 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L nr 281 z 1995 r.).

2 W prawie polskim implementacją dyrektywy 95/46 jest ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922).

3 Czasem miało to nawet miejsce w obrębie tego samego państwa – niemieckie landy.

4 Specjalna ankieta Eurobarometru nr 359 „Ochrona danych i tożsamość elektroniczna w UE (2011)", http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf [dostęp: 29.06.2017].

5 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L 119 z 2016 r.), dalej: RODO lub Rozporządzenie.

prawny będący rozporządzeniem sprawił, że na terenie wszystkich państw członkowskich zaczną obowiązywać bezpośrednio te same przepisy, bez konieczności ich implementacji do krajowego porządku prawnego. Jednakże RODO nie wprowadza harmonizacji pełnej, która rozumiana jest jako zupełne (pełne) uregulowanie danej przedmiotowej sfery, wyłączając dopuszczalność stosowania przepisów krajowych. RODO jest przykładem harmonizacji częściowej, w której pozostawia się państwom UE większą lub mniejszą swobodę w danej dziedzinie po wejściu w życie aktu harmonizującego[6]. W określonych sytuacjach państwa mają możliwość wyboru kierowania się w pewnych sprawach przedmiotowych przepisami unijnymi lub też krajowymi (tzw. harmonizacja fakultatywna)[7]. Jakie zmiany czekają więc kraje członkowskie w związku z nową regulacją i jak w tym wszystkim prezentuje się nowe zagadnienie jakim jest pseudonimizacja?

2. Główne zmiany związane z wejściem Rozporządzenia 2016/679

Rozporządzenie wprowadza wiele nowych rozwiązań prawnych. W pierwszej kolejności należy wskazać na nowe i zwiększone uprawnienia obywateli. Tytułem przykładu jest to tzw. „prawo do bycia zapomnianym"[8], prawo do żądania przeniesienia danych oraz rozszerzone prawo dostępu i wglądu obywatela we własne dane. Ponadto osoby, których dane dotyczą, będą dysponowały wzmocnionym prawem sprzeciwu wobec przetwarzania ich danych, w tym m.in. prawo do zakazania marketingu bezpośredniego z wykorzystaniem danych osobowych, co ma istotne znaczenie w stosunku do firm, które bazują na analityce danych.

Nowością jest również powiadomienie o wycieku danych. Obowiązkiem administratorów danych będzie zgłaszanie w ciągu 72 godzin od wykrycia do właściwego organu nadzoru[9] przypadków naruszeń, które

---

6 J. Osiejewicz, *Harmonizacja prawa państw członkowskich Unii Europejskiej*, Warszawa 2016, s. 59–60.

7 G. Sibiga, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia,* „Monitor Prawniczy" 2016, Legalis.

8 To prawo do usunięcia danych osobowych z bazy danej instytucji. warunkiem jest to, że dane te nie są już dłużej używane.

9 Będzie to generalny inspektor ochrony danych osobowych.

mogą skutkować zagrożeniem praw i swobód osób, których dane naruszono. Ponadto może także wystąpić konieczność zawiadomienia osób, których dane wyciekły (np. klientów). Jak wskazuje Anna Kobylańska[10] to sytuacja, z jaką krajowe przedsiębiorstwa nigdy wcześniej nie miały do czynienia. Zauważa, iż przedsiębiorcy – poza branżą telekomunikacyjną – nie są przyzwyczajeni do zgłaszania własnych naruszeń ochrony danych osobowych organom nadzoru. W związku z tym obowiązek ten wymaga nie tylko zidentyfikowania powstałego naruszenia, ale również wprowadzenia odpowiednich procedur reagowania na incydenty związane z ochrony danych.

Ponadto zaznaczyć należy, że rozbudowany i zaostrzony został system kar pieniężnych. Firmy mogą liczyć się z karami rzędu 20 000 000 euro lub 4% całkowitego rocznego światowego obrotu z poprzedniego roku[11]. Przepisy zaznaczają, że każdy przypadek należy rozpatrywać indywidualnie. W doktrynie wskazuje się, że nałożenie maksymalnej grzywny może spowodować konieczność zakończenia działalności podmiotu[12]. W razie naruszeń przepisów Rozporządzenia, szczególnie w przypadku naruszeń niepodlegających grzywnom administracyjnym, kraje członkowskie określają przepisy o karach mających zastosowanie do takich naruszeń oraz wprowadzą odpowiednie środki konieczne do ich wdrożenia. Kary te mają być skuteczne, proporcjonalne i odstraszające.

Z punktu widzenia obywatela zasadniczą zmianą będzie możliwość złożenia skargi na podmioty przetwarzające ich dane do organów nadzorujących w kraju ich zamieszkania, bez względu na to, gdzie mieści się siedziba danego przedsiębiorcy lub innego podmiotu[13]. Przykładowo jeżeli obywatel Polski będzie chciał zaskarżyć praktykę, bądź też politykę prywatności serwisu społecznościowego Facebook[14], nie będzie musiał

10 W. Maroszek, *RODO, czyli ochrona danych 2.0. Nowe unijne przepisy oznaczają trudności dla przedsiębiorców*, http://biznes.onet.pl/wiadomosci/ue/rodo-gdpr-regulacje-ue-o-ochronie-danych-osobowych-firma/7jmc46 [dostęp: 29.06.2017].

11 W zależności od tego, która kwota będzie wyższa.

12 D. Wociór, *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, Warszawa 2016, Legalis.

13 Art. 56 RODO.

14 Znana jest sytuacja, gdy austriacki student prawa – Max Schrems – wysłał do siedziby serwisu oficjalne pismo z prośbą o udostępnienie mu danych, jakie zostały zgromadzone na jego temat, w czasie gdy posiadał konto na Facebooku. Wniosek został rozpatrzony po jego myśli i dostał w związku z tym płytę CD ze wszystkimi informacjami na temat jego aktywności w serwisie (np. korespondencja ze znajomymi,

w związku z tym kontaktować się z irlandzkim rzecznikiem ochrony danych osobowych – wystarczy wtedy skarga do polskiego Generalnego Inspektora Ochrony Danych Osobowych.

Co więcej, aby przetwarzanie danych było zgodne z wymaganiami RODO i w efektywny sposób chroniło prawa osób, których dane dotyczą, administratorzy danych osobowych mają obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych. Takim środkiem mającym na celu zapewnienie ochrony jest np. pseudonimizacja. Ma ona stanowić skuteczny środek zabezpieczenia danych osobowych o czym mowa będzie w kolejnym rozdziale.

3. Pseudonimizacja

3.1. Pojęcie i istota pseudonimizacji

Na wstępie należy pochylić się nad tym, czym w ogóle jest pseudonimizacja. Art. 4 pkt 5 RODO definiuje proces pseudonimizacji jako: „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, o ile takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej".

Istotą tego procesu jest więc kodowanie polegające na zastępowaniu jednego atrybutu innym atrybutem co nadal umożliwia wyodrębnienie konkretnej osoby fizycznej i tworzenie w odniesieniu do tej osoby powiązań między różnymi zbiorami. W związku z tym nadal istnieje ryzyko pośredniego zidentyfikowania osoby fizycznej z racji tego, że proces pseudonimizacji jest procesem odwracalnym[15].Dlatego też stosowanie samej pseudonimizacji nie będzie skutkowało anonimowym zbiorem danych o czym

czy też posty na jego profilu). Niepokój Schremsa wzbudził fakt, że informacje te były przechowywane na serwerach Facebooka pomimo tego, że nie posiadał on już tam konta. Sprawa wzbudziła zainteresowanie Irlandzkiego Komisarza Ochrony Danych Osobowych, który postanowił przyjrzeć się sprawie.

15 T. Żmijewski, *Fanpage na Facebooku, przetwarzanie danych osobowych, a RODO*, http://blog.e-odo.pl/category/reforma-ochrony-danych-osobowych/anonimizacja-i-pseudonimizacja/ [dostęp: 29.06.2017].

mowa będzie przy porównaniu pseudonimizacji z anonimizacją. Z drugiej jednak strony stosowanie tego rodzaju procedur pozwoli na ograniczenie zagrożenia w stosunku do informacji identyfikujących podmioty. Przepisy RODO podkreślają, iż pseudonimizacja danych osobowych może ograniczyć ryzyko dla osób, których dane dotyczą oraz pomóc administratorom wywiązać się z obowiązku ochrony danych[16]. Jest ona więc procesem pośrednim między anonimizacją a przetwarzaniem danych w postaci jawnej.

Od pseudonimizacji powstało pojęcie danych pseudonimicznych, czyli niezawierających informacji umożliwiających zidentyfikowanie określonej osoby. Przykładem danych pseudonimizowanych może być posługiwanie się wewnętrznym numerem klienta, zamiast jego danymi osobowymi[17]. Nie można więc wtedy przypisać ich do konkretnej osoby fizycznej. Skutkiem stosowania pseudonimizacji może być ograniczenie wystąpienia naruszeń bezpieczeństwa informacji. Należy jednak w tym miejscu zwrócić uwagę na możliwość naruszenia. Mianowice dane, które poddane zostały pseudonimizacji mogą pośrednio doprowadzić do identyfikacji tożsamości osoby, gdy składają się z informacji, które w określonym i ograniczonym środowisku, np. miejscowości, wyróżniają i konkretyzują daną osobę[18]. Jako przykład można wskazać pseudonimizację wyroku sądowego, gdy sprawa rozpatrywana przez sąd jest otwarcie znana i wywołuje emocje w społeczności lokalnej. W takim przypadku pomimo ukrycia danych identyfikacyjnych osoby, które są w nią zaangażowane będą rozpoznawalne.

Dane pseudonimizowane będą w dalszym ciągu danymi osobowymi – proces ten jest jednakże uważany za jeden ze sposobów zabezpieczenia danych osobowych[19]. Z obowiązku, aby dane osobowe dotyczyły podmiotu możliwego do zidentyfikowania wynika, że nie będą stanowiły danych osobowych takie dane, które zostały poddane procedurze anonimizacji, za pomocą pozbawienia ich właściwości umożliwiających połączenie z osobą, której dotyczą[20].

16 Motyw 28 preambuły RODO.

17 Osoba nieupoważniona uzyska więc w takim przypadku dostęp do danych w formie np. ID 36821.

18 M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, Legalis.

19 D. Dörre-Kolasa, *Ochrona danych osobowych pracowników w świetle Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2017, Legalis.

20 *Ibidem*.

Celowość zastosowania procedury pseudonimizacji powinna być brana pod uwagę na etapie projektowania, w części wdrażania zabezpieczeń i rozwiązań informatycznych oraz w sytuacji zmiany celu przetwarzania danych osobowych bez zgody osoby fizycznej. Tytułem przykładu zmiana celu przetwarzania ma miejsce w przypadku, gdy dane zgromadzone zostały celem zawarcia i wykonania umowy, a następnie administrator danych przystępuje do przetwarzania danych w celu przeciwdziałania oszustwom[21].

3.2. Pseudonimizacja a anonimizacja

Przechodząc do porównania procesów pseudonimizacji i anonimizacji należy wskazać, że podstawowa różnica polega na tym, iż skutkiem anonimizacji jest nieodwracalne udaremnienie identyfikacji danej osoby. Anonimizacja pozbawia więc informację charakteru danych osobowych[22]. Z kolei w momencie zastosowania pseudonimizacji nadal występuje prawdopodobieństwo pośredniego ustalenia tożsamości osoby fizycznej. Ponadto, po przeprowadzeniu procesu pseudonimizacji informacje nadal pozostają danymi osobowymi. Pseudonimizację od anonimizacji odróżniać więc będzie trwałość pozbawienia danych możliwości identyfikacji podmiotu[23]. Co ważne nie jest ona metodą anonimizacji.

Przykładem błędnych przekonań związanych z pseudonimizacją jest głośna sprawa wycieku danych z America On Line z 2006 roku. Wtedy to została udostępniona publicznie baza danych zawierająca ok. dwadzieścia milionów słów kluczy, które wpisywane były do wyszukiwarki internetowej przez 685 tysięcy użytkowników w okresie 3 miesięcy – jedynym środkiem maskującym była zamiana identyfikatorów użytkowników AOL skonkretyzowanymi numerami (np. 8247653). Na pierwszy rzut oka wydawać by się mogło, że dane te nie są niebezpieczne. W konsekwencji jednak spowodowało to, iż można było zidentyfikować i zlokalizować niektórych użytkowników. Spseudonimizowane rzędy zapytań wprowadzane w wyszukiwarkach, szczególnie w połączeniu z innymi

21 M. Giersz, *Pseudonimizacja – jak właściwie i skutecznie zapewnić zabezpieczenie danych osobowych*, http://www.rp.pl/Firma/306239993-Pseudonimizacja---jak-wlasciwie-i-skutecznie-zapewnic-zabezpieczenie-danych-osobowych.html#ap-4 [dostęp: 29.06.2017].

22 M. Krzysztofek, *Ochrona…*, *op. cit.*

23 D. Dörre-Kolasa, *Ochrona…*, *op. cit.*

wyróżnikami, takimi jak np. adresy IP lub inne cechy konfiguracyjne klienta, posiadają znaczną moc identyfikacji[24].

3.3. Obowiązek pseudonimizacji

Metoda realizacji obowiązku pseudonimizacji określona została w art. 25 RODO, zgodnie z którym, przy uwzględnieniu:

1) stanu wiedzy technicznej,
2) kosztów wdrażania,
3) charakteru, zakresu, kontekstu i celu przetwarzania oraz
4) ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania

– administrator, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, zobligowany jest do wdrożenia odpowiednich środków technicznych i organizacyjnych, takich jak pseudonimizacja, zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak, aby spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

Ponadto w stosunku do domyślnego przetwarzania danych osobowych przewidziano regulację, zgodnie z którą administrator powinien wdrożyć stosowne środki techniczne i organizacyjne, aby domyślnie przetwarzane były tylko te dane osobowe, które są konieczne dla osiągnięcia każdego konkretnego celu przetwarzania.

Zgodnie z art. 25 ust. 2 zdanie drugie obowiązek ten odnosi się do:

1) liczby zbieranych danych osobowych,
2) zakresu ich przetwarzania,
3) okresu ich przechowywania,
4) ich dostępności.

Szczególnie środki te powinny zagwarantować, aby domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. Spełnienie powyższych obowiązków będzie

24 *Opinia Grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych 05/2014 w sprawie technik anonimizacji*, http://www.univers.com.pl/storage/news/pseudonimizacja_danych_osobowych_wedlugo_rodo_f0woo.pdf [dostęp: 29.06.2017].

mogło być wykazane przez administratora m.in. przez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42 RODO.

Warto również w tym miejscu wskazać na regulację art. 24 ust. 2 RODO. Mianowicie istnienie obowiązku wdrożenia przez administratora odpowiednich polityk ochrony danych uzależnione zostało od przesłanki proporcjonalności w stosunku do czynności przetwarzania. Będzie to miało miejsce najczęściej w przypadku małych przedsiębiorstw. Nie oznacza to jednak oczywiście zwolnienia z obowiązku prowadzenia jakiejkolwiek dokumentacji z zakresu ochrony danych osobowych.

Co równie istotne, zasady ochrony danych wynikające z przepisów Rozporządzenia nie będą mieć zastosowania do[25]:

- informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną oraz
- danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować.

Rozporządzenie nie dotyczy przetwarzania anonimowych informacji, w tym przetwarzania do celów statystycznych lub naukowych.

3.4. Metody pseudonimizacji – wybrane przykłady

W Opinii Grupy Roboczej wymieniono kilka przykładowych metod pseudonimizacji, które mogą stanowić pewnego rodzaju wskazówki i wytyczne dla podmiotów, które zobowiązane będą do jej stosowania. Do najczęściej stosowanych technik należą:

- tzw. szyfrowanie z kluczem tajnym – posiadacz klucza może bez trudu ponownie określić każdą osobę, której dane dotyczą, za pomocą odszyfrowanie zbioru danych. Jest to możliwe z uwagi na to, że dane osobowe w dalszym ciągu znajdują się w tym zbiorze danych, aczkolwiek w zaszyfrowanej formie.
- funkcja skrótu – polega na tym, że skraca się dane osobowe do danych wartości, np. numer i adres zamieszkania podlega skróceniu do pierwszych liter miejscowości i ulicy, albo imię i nazwisko do inicjałów.
- tokenizacja – sposób ten jest zwykle używany w sektorze finansowym celem zastąpienia numerów identyfikacyjnych kart cechami, które ograniczają przydatność dla atakującego. Polega ona

25 Motyw 26 preambuły RODO.

zazwyczaj na stosowaniu mechanizmów szyfrowania jednokierunkowego lub na przypisaniu, przy pomocy funkcji indeksu, sekwencji liczb lub losowo wygenerowanych liczb, które nie zostały w sposób matematyczny uzyskane z danych pierwotnych.

3.5. Wady pseudonimizacji na wybranych przykładach

Mimo, wydawać by się mogło, skuteczności procesu pseudonimizacji jako środka zabezpieczenia danych osobowych Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych wskazuje na kilka wad powyższej procedury na podstawie wybranych kazusów.

Pierwszy z nich odnosi się do sieci społecznościowych. Wykazano w stosunku do nich[26], że szczególnie chronione dane na temat pewnych osób fizycznych można uzyskać z grafów powiązań społecznościowych, pomimo zastosowania technik pseudonimizacji do takich danych. Przedstawiciel sieci społecznościowej mylnie przypuszczał, że pseudonimizacja była wystarczającym środkiem, który zapobiegnie ustaleniu tożsamości po sprzedaży danych innym firmom do celów reklamowych i marketingowych. W miejsce prawdziwych nazwisk dostawca wykorzystał pseudonimy, jednakże nie przyczyniło się to do anonimizacji użytych profili z uwagi na to, że powiązania między różnymi osobami fizycznymi są unikatowe i mogą zostać użyte jako identyfikatory.

Drugi natomiast dotyczy zagadnienia lokalizacji. Mianowicie badacze z Instytutu Technologii w Massachusetts[27] przeprowadzili analizę zbioru danych opatrzonych pseudonimem składającego się z danych z 15 miesięcy przedstawiających współrzędne dotyczące czasowej mobilności przestrzennej 1,5 miliona ludzi na obszarze o promieniu 100 kilometrów. Dowiedli oni, że przy pomocy czterech punktów lokalizacji można wydzielić dziewięćdziesiąt pięć procent populacji i że tylko dwa punkty wystarczyły, by wyróżnić ponad pięćdziesiąt procent osób, których dane dotyczą (co ważne jeden z tych punktów jest znany i jest to przypuszczalnie „biuro" lub „dom"), w znacznym stopniu zmniejszając ochronę prywatności pomimo tego, że tożsamości poszczególnych osób zostały opatrzone pseudonimem przez zastąpienie ich prawdziwych cech innymi oznaczeniami.

26 A. Narayanan and V. Shmatikov, *De-anonymizing social networks*, [w:] *30th IEEE Symposium on Security and Privacy*, 2009.

27 Y.-A. de Montjoye, C. Hidalgo, M. Verleysen i V. Blondel, *Unique in the Crowd: The privacy bounds of human mobility*, „Nature" 2013, nr 1376.

Wskazać tu można również na kazus omawiany wcześniej, który dotyczył możliwość zidentyfikowania danej osoby w konkretnym środowisku. W związku z powyższym należy pamiętać, że pseudonimizacja ogranicza jedynie sposobność połączenia danego zbioru danych z prawdziwą tożsamością osoby, której informacje dotyczą. Dlatego też wciąż istnieje szansa, że w przypadku zastosowania tej techniki możliwa będzie identyfikacja.

4. Odpowiedzialność w świetle rozporządzenia unijnego i prawo do odszkodowania

Istotną zmianą będzie możliwość dochodzenia odszkodowania przez osoby fizyczne za poniesioną szkodę w związku z naruszeniem przepisów Rozporządzenia przez podmioty, które przetwarzają dane. Jest to wyjście naprzeciw prawom osób, których dane dotyczą z uwagi na to, że obecne przepisy nie przewidują takiej konstrukcji[28].

Każda osoba, która poniosła szkodę majątkową lub niemajątkową z powodu niezgodnego z RODO przetwarzania danych, ma prawo uzyskania od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

Przepisy Rozporządzenia nakładają na administratora odpowiedzialność za szkody wywołane niezgodnym z prawem przetwarzaniem danych osobowych. Jednakże co należy wskazać, podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem tylko w sytuacji, gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmiot przetwarzający lub też wówczas, gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom[29].

Administrator, jak też podmiot przetwarzający powinni zostać zwolnieni od odpowiedzialności, gdy udowodnią brak swojej winy w wystąpieniu faktu, który spowodował powstanie szkody[30]. Natomiast jeśli w tym samym przetwarzaniu bierze udział więcej niż jeden administrator lub podmiot przetwarzający lub też uczestniczy w nim zarazem administrator, jak

---

28 Do tej pory dochodzenie odszkodowania przez osoby fizyczne na drodze cywilnej możliwe było na podstawie ogólnych przepisów ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tj. Dz.U. 2017 poz. 459), dalej: k.c.

29 Art. 82 ust. 2 RODO.

30 Motyw 146 preambuły RODO.

i podmiot przetwarzający, to odpowiadają prawnie za szkodę spowodowaną przetwarzaniem i ponoszą solidarną odpowiedzialność za całą szkodę.

Każdy administrator lub podmiot przetwarzający, który wypłacił pełne odszkodowanie za spowodowaną szkodę, posiada roszczenie regresowe w stosunku do pozostałych administratorów lub podmiotów przetwarzających, którzy brali udział w tym samym przetwarzaniu. Postępowanie sądowe co do korzystania z prawa do odszkodowania wszczynane jest przed sądem właściwym na mocy prawa krajowego państwa członkowskiego.

5. RODO w aspekcie praktycznym

Na zakończenie należałoby się również odnieść do globalnego badania przeprowadzonego przez firmę Dell[31], które dotyczyło omawianego Rozporządzenia[32]. Badanie pokazało, że przedsiębiorstwa nie są świadome wymogów nakładanych na nie przez nowe regulacje unijne i nie wiedzą, jak dostosować się do regulacji. Wynika z niego, że ponad osiemdziesiąt procent przedstawicieli firm, którzy wzięli udział w badaniu, ma znikomą wiedzę lub nie wie zupełnie nic na temat RODO. Z kolei prawie siedemdziesiąt procent respondentów stwierdza, iż nie są jeszcze przygotowani na RODO lub nie wiedzą nic o stanie przygotowania swojej firmy. Zaledwie trzy procent ankietowanych zadeklarowało, że ich firma ma odpowiedni plan wprowadzenia Rozporządzenia.

Jak wskazują wyniki badań, firmy zdają sobie sprawę z tego, że nieprzestrzeganie nowych przepisów będzie miało wpływ na poziom bezpieczeństwa danych, jak również i na rezultaty biznesowe. Przedsiębiorstwa nie są jednak pewne zakresu koniecznych zmian, wymiaru sankcji za nieprzestrzeganie

---

31 W badaniu wzięło udział 821 specjalistów ds. biznesowych i IT, którzy odpowiedzialni są za ochronę danych w firmach mających klientów w całej Europie. Ankietowani odpowiadali na pytania odnoszące się do świadomości i odbierania przepisów RODO, przygotowania na ich wejście w życie w 2018 roku oraz spodziewanych następstw ich naruszenia. Badanie przeprowadzone było w Stanach Zjednoczonych, Kanadzie, regionie Azji i Pacyfiku (Australia, Hongkong, Singapur, Indie), Niemczech, Belgii, Holandii, Wielkiej Brytanii, Szwecji, Włoszech, Hiszpanii, Francji i Polsce. Ankietę wypełnił także zespół zarządzający z przedsiębiorstw, które zatrudniają poniżej 100 pracowników.

32 *Badanie firmy Dell: przedsiębiorstwa nie są gotowe na GDPR – nowe unijne rozporządzenie o ochronie danych*, http://www.dell.com/learn/pl/pl/plcorp1/press-releases/2016-10-20-dell-research-for-gdpr [dostęp: 29.06.2017].

regulacji i ich wpływu na przedsiębiorstwo. Siedemdziesiąt dziewięć procent respondentów stwierdziło, że nie wie, czy ich przedsiębiorstwa zostałyby ukarane, lub sądzi, że nie dotknęłaby ich kara za stosowane podejście do ochrony danych, gdyby przepisy RODO obowiązywały w tym roku.

Ponad dziewięćdziesiąt procent badanych stwierdziło, że aktualne procedury w ich przedsiębiorstwach nie spełniają wymogów RODO. Widać więc jak niski odsetek firm przygotowany jest na wejście nowej regulacji prawnej.

6. Zakończenie

Wprowadzenie nowego pojęcia, jakim jest pseudonimizacja, należy uznać za pozytywną zmianę. Wcześniej bowiem prawo nie zauważało takich danych, które wszakże pojawiają się co raz częściej wraz z rozwojem technologii i postępującej informatyzacji. Warto jednak również pamiętać o tym, że wszelkie procesy związane z postępem technologicznym niosą za sobą szereg zagrożeń wynikających np. z ataków hakerskich. W związku z tym konieczne jest opracowanie takich procedur, które skutecznie będą mogły zabezpieczyć nasze dane. Wydaje się, że pseudonimizacja spełnia takie wymagania.

Pozytywnie można ocenić także kwestię uregulowania odpowiedzialności prawnej i prawa do odszkodowania na poziomie rozporządzenia. Dotychczas domaganie się odszkodowania przez osoby fizyczne na drodze cywilnoprawnej było co prawda możliwe na gruncie przepisów ogólnych k.c., jednakże judykatura podchodziła do takich spraw dosyć powściągliwie. Ponadto świadomość obywateli o możliwości dochodzenia takiego odszkodowania była znikoma. Rozporządzenie natomiast wprost przewiduje taką możliwość i to zarówno za szkodę majątkową, jak i niemajątkową. Oznacza to, że dochodzenie zadośćuczynienia pieniężnego, np. za niezgodne z prawem ujawnienie naszych danych osobowych będzie dużo łatwiejsze.

Odnosząc się do świadomości przedsiębiorstw w związku z planowanym wejściem w życie RODO można zauważyć, że część przepisów wciąż rodzi pytania, a większość firm nie zaczęła nawet przygotowywać się do nowych regulacji. Ponadto również trzeba mieć na uwadze to, że poza unijnymi przepisami, w życie wejdzie także nowa polska ustawa[33].

---

33 *Ustawa o ochronie danych osobowych – projekt roboczy*, https://www.gov.pl/documents/31305/0/projekt_ustawy_o_ochronie_danych_osobowych_28.03.2017.pdf/87757e91-129f-89a5-b442-0e17f9d05245 [dostęp: 29.06.2017].

Przedsiębiorstwa mają więc niecały rok na dostosowanie systemów i procedur do przepisów unijnych.

Bibliografia

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.Urz. UE L 119 z 2016 r.).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922).

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tj. Dz.U. 2017 poz. 459).

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE l nr 281 z 1995 r.).

Literatura

V. Blondel Y.-A. de Montjoye, C. Hidalgo i M. Verleysen, *Unique in the Crowd: The privacy bounds of human mobility*, Nature, nr 1376, 2013.

D. Dörre-Kolasa, *Ochrona danych osobowych pracowników w świetle Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2017.

M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016.

A. Narayanan and V. Shmatikov, *De-anonymizing social networks*, [w:] *30th IEEE Symposium on Security and Privacy*, 2009.

J. Osiejewicz, *Harmonizacja prawa państw członkowskich Unii Europejskiej*, Warszawa 2016.

G. Sibiga, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia,* „Monitor Prawniczy" 2016.

D. Wociór, *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, Warszawa 2016.

Źródła internetowe

Specjalna ankieta Eurobarometru nr 359 „Ochrona danych i tożsamość elektroniczna w UE (2011)", http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf [dostęp: 29.06.2017].

W. Maroszek, *RODO, czyli ochrona danych 2.0. Nowe unijne przepisy oznaczają trudności dla przedsiębiorców*, http://biznes.onet.pl/wiadomosci/ue/rodo-gdpr-regulacje-ue-o-ochronie-danych-osobowych-firma/7jmc46 [dostęp: 29.06.2017].

T. Żmijewski, *Fanpage na Facebooku, przetwarzanie danych osobowych, a RODO*, http://blog.e-odo.pl/category/reforma-ochrony-danych-osobowych/anonimizacja-i-pseudonimizacja/ [dostęp: 29.06.2017].

M. Giersz, *Pseudonimizacja – jak właściwie i skutecznie zapewnić zabezpieczenie danych osobowych*, http://www.rp.pl/Firma/306239993-Pseudonimizacja---jak-wlasciwie-i-skutecznie-zapewnic-zabezpieczenie-danych-osobowych.html#ap-4 [dostęp: 29.06.2017].

Opinia Grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych 05/2014 w sprawie technik anonimizacji, http://www.univers.com.pl/storage/news/pseudonimizacja_danych_osobowych_wedlugo_rodo_f0woo.pdf [dostęp: 29.06.2017].

Badanie firmy Dell: przedsiębiorstwa nie są gotowe na GDPR – nowe unijne rozporządzenie o ochronie danych, http://www.dell.com/learn/pl/pl/plcorp1/press-releases/2016-10-20-dell-research-for-gdpr [dostęp: 29.06.2017].

Ustawa o ochronie danych osobowych – projekt roboczy, https://www.gov.pl/documents/31305/0/projekt_ustawy_o_ochronie_danych_osobowych_28.03.2017.pdf/87757e91-129f-89a5-b442-0e17f9d05245 [dostęp: 29.06.2017].

Abstrakt

Pseudonimizacja jako nowy środek zabezpieczenia danych osobowych w świetle zmian prawnych w UE – wybrane aspekty

W niniejszym artykule zajęto się kwestią pseudonimizacji, która stanowi sposób zabezpieczenia danych osobowych. 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. Pojęcie to pojawia się po raz pierwszy w nowym rozporządzeniu unijnym z 2016 roku.

W artykule przedstawiono główne zmiany związane z nową regulacją, opisano proces pseudonimizacji jak i wybrane metody jej stosowania. Zaprezentowano także wady, które mogą się wiązać z tą techniką. Autor odnosi się również do aspektu praktycznego przytaczając wyniki badania prowadzonego na zlecenie firmy Dell w 2016 roku dotyczącego nowego rozporządzenia.

SŁOWA KLUCZOWE: pseudonimizacja, ochrona danych osobowych, rozporządzenie, nowelizacja, RODO.