GRUPA ROBOCZA DS. OCHRONY DANYCH POWOŁANA NA MOCY ART. 29

01248/07/PL
WP 136

Opinia 4/2007 w sprawie pojęcia danych osobowych

przyjęta w dniu 20 czerwca

Niniejsza grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym
w zakresie ochrony danych i prywatności, którego zadania określają przepisy art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Sekretariat grupy mieści się przy dyrekcji C (Sądownictwo Cywilne, Prawa Podstawowe i Obywatelstwo) Dyrekcji Generalnej ds. Sprawiedliwości, Wolności i Bezpieczeństwa Komisji Europejskiej,
B-1049 Bruksela, Belgia, biuro nr LX-46 01/43.

Strona internetowa: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

powołana na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.[1],

uwzględniając art. 29 i art. 30 ust. 1 lit. a) i ust. 3 tej dyrektywy i art. 15 ust. 3 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r.,

uwzględniając art. 255 Traktatu WE i rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

[1] Dziennik Urzędowy L 281 z 23.11.1995, str. 31, dostępny na stronie internetowej: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. WSTĘP

Grupa robocza jest świadoma potrzeby przeprowadzenia dogłębnej analizy pojęcia danych osobowych. Informacje o praktykach panujących w państwach członkowskich UE świadczą o istnieniu niepewności, a także o występowaniu praktycznych rozbieżności pomiędzy państwami członkowskimi w zakresie ważnych elementów tego pojęcia, które mogą niekorzystnie wpływać na prawidłowe funkcjonowanie istniejącego systemu ochrony danych w różnych sytuacjach. Rezultat analizy pojęcia mającego kluczowe znaczenie przy stosowaniu i wykładni przepisów dotyczących ochrony danych z pewnością w dużym stopniu wpłynie na wiele istotnych kwestii, szczególnie na zagadnienia takie jak zarządzanie tożsamością w kontekście e-administracji i e-zdrowia oraz w kontekście identyfikacji radiowej (RFID).

Niniejsza opinia grupy roboczej ma na celu wypracowanie wspólnej koncepcji danych osobowych, jak również ustalenie sytuacji, w których należy stosować ustawodawstwo krajowe dotyczące ochrony danych oraz określenie sposobu jego stosowania. Opracowanie wspólnej definicji pojęcia danych osobowych jest warunkiem ustalenia zakresu stosowania przepisów dotyczących ochrony danych. Następstwem tych prac ma być sformułowanie wytycznych na temat sposobu stosowania ustawodawstwa krajowego w dziedzinie ochrony danych w odniesieniu do pewnych sytuacji występujących w całej Europie, aby w ten sposób przyczynić się do jednolitego stosowania norm, co jest główną funkcją grupy roboczej powołanej na mocy art. 29.

Analizę zawartą w niniejszym dokumencie ilustrują przykłady z krajowej praktyki europejskich organów ds. ochrony danych. Większość przykładów zredagowano jednak na użytek niniejszego dokumentu.

II. UWAGI OGÓLNE I KWESTIE DOTYCZĄCE POLITYKI

Dyrektywa zawiera szeroką definicję danych osobowych

Definicja danych osobowych zawarta w dyrektywie 95/46/WE (zwanej dalej „dyrektywą o ochronie danych" lub „dyrektywą") brzmi następująco:

„'dane osobowe' oznacza wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość".

Należy odnotować, że definicja ta jest ze strony prawodawcy europejskiego wyrazem woli przyjęcia szerokiej koncepcji „danych osobowych", którą tą wolę podtrzymywano przez cały czas trwania procedury prawodawczej. W pierwotnym wniosku Komisja wyjaśniała, że „podobnie jak w Konwencji 108, przyjęto szeroką definicję uwzględniającą wszelkie informacje mogące dotyczyć danej osoby"[2]. W zmienionym wniosku Komisja stwierdziła, że „zmieniony wniosek uwzględnia życzenie Parlamentu, aby definicja „danych osobowych" była jak najogólniejsza, tak aby uwzględnić wszystkie informacje dotyczącej osoby możliwej do zidentyfikowania";[3], życzenie to wzięła pod uwagę również Rada, ustanawiając wspólne stanowisko[4].

Celem przepisów zawartych w dyrektywie jest ochrona osób fizycznych.

Artykuł 1 dyrektywy 95/46/WE i art. 1 dyrektywy 2002/58/WE jasno określają nadrzędny cel zawartych w nich przepisów: chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych. Jest to bardzo istotna informacja, którą należy mieć na uwadze przy wykładni i podczas stosowania przepisów obu tych aktów. Może ona odgrywać znaczącą rolę przy określaniu, w jaki sposób należy stosować przepisy dyrektywy w wielu sytuacjach, w których prawa osób fizycznych nie są zagrożone, a także zapobiegać takiej wykładni tychże przepisów, która pozbawiłaby osoby fizyczne ochrony ich praw.

Zakres stosowania dyrektywy wyklucza szereg czynności, a tekst cechuje pewna elastyczność mająca na celu odpowiednie dostosowanie uregulowania do okoliczności

Mimo szerokiej koncepcji „danych osobowych" i „przetwarzania", zawartej w dyrektywie, sam fakt, iż dana sytuacja może zostać uznana za wiążącą się z „przetwarzaniem danych osobowych" w świetle definicji, nie przesądza o stosowaniu przepisów dyrektywy, w szczególności przepisów art. 3. Oprócz wyłączeń związanych z zakresem prawa Wspólnoty, wyłączenia na mocy art. 3 uwzględniają również sposób przetwarzania (sposób ręczny i niezorganizowany) i cel wykorzystania (przez osobę fizyczną do czynności o charakterze czysto osobistym lub domowym). Nawet w przypadku, gdy mamy do czynienia z przetwarzaniem danych osobowych w zakresie przewidzianym w dyrektywie, część zawartych w niej przepisów może nie stosować się do danego przypadku. Szereg przepisów dyrektywy cechuje znaczny stopień elastyczności, mający na celu zachowanie odpowiedniej równowagi pomiędzy ochroną praw osoby, której dotyczą dane, z jednej strony, a uzasadnionymi interesami

---

2 COM (90) 314 final, 13.9.1990, str. 19 (uwaga dotycząca art. 2)

3 COM (92) 422 final, 28.10.1992, str. 10 (uwaga dotycząca art. 2)

4 Wspólne stanowisko (WE) nr 1/95, przyjęte przez Radę dnia 20 lutego 1995 r., Dz.U C 93 z 13.4.1995, str.20

administratorów danych, osób trzecich i oraz ewentualnie interesem publicznym z drugiej strony. Przykłady takich przepisów znajdują się w art. 6 (uzależnienie długości okresu przechowywania od konieczności zachowania danych), w art. 7 lit. f) (równowaga interesów pozwalająca uzasadnić przetwarzanie), w art. 10 lit c), ostatni akapit i w art. 11 ust 1 lit c) (przekazywanie informacji osobie, której dotyczą dane, jeżeli jest to konieczne w celu zagwarantowania rzetelnego przetwarzania danych), lub w art. 18 (zwolnienia z obowiązku zawiadomienia), by wymienić tylko niektóre z nich.

Nie należy nadmiernie rozszerzać zakresu przepisów dotyczących ochrony danych.

Niepożądane byłoby stosowanie przepisów dotyczących ochrony danych w sytuacjach, do których nie miały się one stosować i do których nie przeznaczył ich prawodawca. Wymienione powyżej wyłączenia rzeczowe z tytułu art.3, jak również objaśnienia zawarte w motywach 26 i 27 dyrektywy zawierają wskazówki co do sposobu stosowania ochrony danych, do jakiego zmierzał prawodawca.

Jedno z ograniczeń dotyczy sposobu przetwarzania danych. Warto przypomnieć, że przyjęcie w latach siedemdziesiątych pierwszych ustaw o ochronie danych spowodowane było tym, że nowa technologia cyfrowego przetwarzania danych pozwoliła na szybszy i szerszy dostęp do danych osobowych, niż tradycyjne formy ich przetwarzania. W związku z tym ochrona danych na mocy dyrektywy ma na celu ochronę danych przetwarzanych w sposób, który zwiększa ryzyko „łatwego dostępu do danych" (motyw 27). Przetwarzanie danych w sposób niezautomatyzowany wchodzi w zakres dyrektywy tylko wtedy, jeżeli dane te stanowią część zbioru danych lub mają stanowić część takiego zbioru (art. 3).

Inne ograniczenie stosowania ochrony danych ustanowionej przez dyrektywę dotyczy przetwarzania danych w okolicznościach, w których „nie można posłużyć się" sposobami zidentyfikowania osoby, której dane dotyczą (motyw 26), która to kwestia zostanie omówiona w dalszej kolejności.

Należy również unikać nadmiernie zwężającej interpretacji pojęcia danych osobowych.

W przypadkach, w których mechaniczne stosowanie wszystkich przepisów dyrektywy prowadziłoby ewidentnie do zbyt uciążliwych lub nawet absurdalnych rezultatów, należy najpierw sprawdzić, 1) czy sytuacja mieści się w zakresie stosowania dyrektywy, szczególnie zgodnie z jej art. 3; i 2) jeżeli sytuacja objęta jest zakresem jej stosowania, czy dyrektywa lub też przyjęte na jej podstawie ustawodawstwo krajowe nie przewiduje zwolnień lub uproszczeń umożliwiających odpowiednie potraktowanie poszczególnych sytuacji, zapewniające ochronę praw osób fizycznych i wchodzących w grę interesów. Nie należy więc raczej nadmiernie zawężać interpretacji definicji danych osobowych, lecz mieć na uwadze znaczną elastyczność dopuszczalną w stosowaniu przepisów do danych.

Krajowe organy nadzoru ochrony danych odgrywają w tej dziedzinie zasadniczą rolę w ramach swojej misji monitorowania stosowania prawa dotyczącego ochrony danych, która obejmuje wykładnię przepisów prawnych i konkretne wytyczne dla administratorów danych i osób, których dane dotyczą. Powinny one propagować wystarczająco szeroką definicję, która uwzględniałaby zmiany i wszelkie „szare strefy" w swoim zakresie, wykorzystując przy tym odpowiednio elastyczność dyrektywy. Tekst dyrektywy zachęca do kształtowania polityki, która łączyłaby szeroką

interpretację pojęcia danych osobowych z odpowiednią równowagą przy stosowaniu przepisów dyrektywy.

III. ANALIZA DEFINICJI „DANYCH OSOBOWYCH" WEDŁUG DYREKTYWY O OCHRONIE DANYCH

Definicja zawarta w dyrektywie składa się z czterech podstawowych elementów, które na potrzeby niniejszego dokumentu zostaną przeanalizowane osobno. Są to następujące elementy:

- „wszelkie informacje"
- „dotyczące"
- „zidentyfikowanej lub możliwej do zidentyfikowania"
- „osoby fizycznej".

Te cztery podstawowe elementy są ze sobą ściśle związane i wzajemnie się na sobie opierają. Jednakże ze względu na metodologię przyjętą w niniejszym dokumencie każdy z nich zostanie rozpatrzony osobno.

1. PIERWSZY ELEMENT: „WSZELKIE INFORMACJE"

Zawarty w dyrektywie termin „wszelkie informacje" wskazuje jasno, że zamiarem prawodawcy było ustanowienie szerokiego pojęcia danych osobowych. Sformułowanie to wymaga szerokiej interpretacji.

Jeśli chodzi o charakter informacji, pojęcie danych osobowych obejmuje wszelkie stwierdzenia na temat osoby. Obejmuje ono informacje „obiektywne", takie jak obecność pewnych substancji w czyjejś krwi, a także informacje „subiektywne", opinie lub oceny. Ten ostatni rodzaj stwierdzeń dotyczy w znacznym stopniu przetwarzania danych osobowych w sektorach takich jak bankowość, przy ocenie rzetelności dłużników („Tytus jest rzetelnym dłużnikiem"), ubezpieczenia („Nie przewiduje się rychłej śmierci Tytusa") lub też zatrudnienie („Tytus jest dobrym pracownikiem i zasługuje na awans").

Aby stanowić „dane osobowe", informacja nie musi być prawdziwa ani sprawdzona. Przepisy dotyczące ochrony danych uwzględniają ewentualność, że informacje nie są prawdziwe i zapewniają osobie, której dotyczą dane, prawo dostępu do informacji i zakwestionowania ich przy pomocy odpowiednich środków[5].

Jeśli chodzi o treść informacji, pojęcie danych osobowych obejmuje dane zawierające wszelkie rodzaje informacji. Obejmuje ono dane osobowe uznane za „dane szczególnie chronione" w art. 8 dyrektywy, z uwagi na ich szczególnie ryzykowny charakter, ale także bardziej ogólne rodzaje informacji. Termin „dane osobowe" obejmuje informacje dotyczące życia prywatnego i rodzinnego sensu stricto danej osoby, ale także informacje dotyczące wszelkich działań przez nią podejmowanych, takich jak informacje dotyczące relacji zawodowych lub też zachowań ekonomicznych albo

[5] Sprostowania można dokonać, dodając kontrastujące uwagi lub stosując odpowiednie środki prawne, takie jak środki odwoławcze.

społecznych osoby. Obejmuje ono zatem informacje o osobach niezależnie od ich pozycji lub stanowiska (jako konsument, pacjent, pracownik, klient itp.).

Przykład nr 1: Zwyczaje i praktyki zawodowe
Informacje o przepisywanych lekach (np. numer identyfikacyjny leku, nazwa leku, siła leku, wytwórca, cena sprzedaży, nowa recepta lub powtórzenie, powody użycia, powody zakazu zamiany na inny lek, imię i nazwisko lekarza przepisującego, numer telefonu itp.), w postaci indywidualnej recepty lub tez w postaci schematów utworzonych na podstawie wielu recept, mogą być uważane za dane osobowe lekarza przepisującego lek, nawet jeśli pacjent jest anonimowy. W związku z tym dostarczanie informacji o receptach wypisanych przez zidentyfikowanego lub możliwego do zidentyfikowania lekarza producentom przepisanych leków stanowi przekazywanie danych osobowych odbiorcom będącym osobami trzecimi w rozumieniu dyrektywy.

Wykładnię tę potwierdza sformułowanie użyte w dyrektywie. Po pierwsze należy uważać, że pojęcie życia prywatnego i rodzinnego jest szerokie, jak jasno wskazał Europejski Trybunał Praw Człowieka[6]. Po drugie przepisy o ochronie danych osobowych wykraczają poza ochronę szeroko pojętego prawa do poszanowania życia prywatnego i rodzinnego. Należy zaznaczyć, że Karta praw podstawowych Unii Europejskiej traktuje ochronę danych osobowych zapisaną w art. 8 jako prawo niezależne, odrębne i odmienne od prawa do życia prywatnego wymienionego w art. 7 oraz że sytuacja prezentuje się podobnie na poziomie krajowym w niektórych państwach członkowskich. Podejście to potwierdza art. 1 ust. 1, zgodnie z którym celem jest ochrona „podstawowych praw i wolności osób fizycznych, *w szczególności* [lecz nie wyłącznie] ich prawa do prywatności". Dyrektywa zawiera zresztą osobne odniesienie do przetwarzania danych osobowych w kontekście innym niż domowy i rodzinny, na przykład w kontekście określonym przez przepisy prawa pracy (art. 8 ust. 2 lit. b), wyrok skazujący, sankcje administracyjne lub orzeczenia w sprawach cywilnych (art. 8 ust. 5) lub marketing bezpośredni (art. 14 lit. b). Europejski Trybunał Sprawiedliwości[7] wyraził poparcie dla tego szerokiego podejścia.

Jeśli chodzi o format informacji lub o nośnik, pojęcie danych osobowych obejmuje informacje dostępne w jakiejkolwiek formie, na przykład alfabetycznej, liczbowej, graficznej, fotograficznej lub akustycznej. Obejmuje ono informacje zapisane na papierze oraz informacje zapisane w pamięci komputerowej za pomocą kodu dwójkowego, lub też na przykład na kasecie wideo. Wynika to w sposób logiczny z faktu, że zautomatyzowane przetwarzanie danych wchodzi w zakres pojęcia. W szczególności dane dźwiękowe oraz obrazowe zaliczają się do danych osobowych, jako że mogą one zawierać informacje na temat osoby fizycznej. W związku z tym osobne odniesienie do danych dźwiękowych i obrazowych w art. 33 dyrektywy należy

[6] Wyrok Europejskiego Trybunału Praw Człowieka w sprawie Amman przeciwko Szwajcarii z dnia 16.2.2000 r., § 65: „[…] termin „życie prywatne" nie może być interpretowany w sposób zawężający. W szczególności, poszanowanie życia prywatnego obejmuje prawo do nawiązywania i rozwijania relacji z innymi ludźmi; ponadto nic nie uzasadnia wykluczenia czynności o charakterze zawodowym lub handlowym z zakresu pojęcia „życie prywatne" (patrz wyrok w sprawie Niemietz przeciwko Niemcom z dnia 16 grudnia 1992 r., seria A nr 251-B, str. 33-34, § 29 oraz wyrok w sprawie Halford, cytowany powyżej, str. 1015-16, § 42). Ta szeroka interpretacja jest zgodna z konwencją Rady Europy z dnia 28 stycznia 1981 r. [...]"

[7] Wyrok Europejskiego Trybunału Sprawiedliwości C-101/2001 z dnia 6.11.2003 r. (Lindqvist), § 24: „Termin dane osobowe użyty w art. 3 ust. 1 dyrektywy 95/46 obejmuje, zgodnie z definicją zawartą w jej art. 2 lit. a), wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Termin ten obejmuje niewątpliwie nazwisko osoby w połączeniu z jej danymi telefonicznymi lub informacjami o jej warunkach pracy lub zainteresowaniach".

rozumieć jako potwierdzenie i wyjaśnienie, że ten rodzaj danych mieści się w jej zakresie stosowania (jeżeli spełnione są wszystkie pozostałe warunki) i że dyrektywa stosuje się do nich. Założenie to jest logiczne w stosunku do tego przepisu, dotyczącego oceny tego, czy przepisy dyrektywy zapewniają odpowiednie uregulowanie w tych obszarach. Jest to dodatkowo wyjaśnione w motywie 14, który stanowi że „w ramach społeczeństwa informacyjnego ma znaczenie rozwój technik gromadzenia, przekazywania, kompilowania, rejestrowania, przechowywania i przesyłania danych dźwiękowych i obrazowych osób fizycznych, niniejsza dyrektywa powinna mieć zastosowanie do przetwarzania takich danych". Dodatkowo informacja może być częścią zorganizowanej bazy danych lub zbioru, nawet jeżeli nie jest uznawana za dane osobowe. Również informacje zawarte w tekście dokumentu elektronicznego mogą zostać uznane za dane osobowe, jeżeli spełnione są inne kryteria zawarte w definicji danych osobowych. Przykładowo poczta elektroniczna może zawierać „dane osobowe".

Przykład nr 2: Bankowe usługi telefoniczne:

W kontekście bankowych usług telefonicznych, jeżeli instrukcje głosowe klienta nagrywane są na taśmę, te nagrane instrukcje należy uważać za dane osobowe.

Przykład nr 3: Nadzór wideo

Obrazy osób zarejestrowane przez system nadzoru wideo mogą stanowić dane osobowe, jeżeli można rozpoznać te osoby.

Przykład nr 4: rysunek dziecka

W wyniku testu neurologiczno-psychiatrycznego przeprowadzonego na dziewczynce w czasie postępowania sądowego w sprawie opieki nad nią, przedłożono sporządzony przez nią rysunek przedstawiający jej rodzinę. Rysunek zawiera informacje o nastroju dziewczynki oraz o jej odczuciach w stosunku do różnych członków jej rodziny. W związku z tym należy go uważać za „dane osobowe". Rysunek ujawni informacje dotyczące dziecka (jego stan zdrowia z punktu widzenia psychiatrycznego) a także np. zachowania jej ojca lub matki. W przypadku tym rodzice mogą więc skorzystać z prawa dostępu do tej konkretnej informacji.

Szczególny nacisk należy położyć na dane biometryczne. Dane te można zdefiniować jako właściwości biologiczne, cechy fizjologiczne, cechy życiowe lub powtarzalne czynności, przy czym te cechy i/lub czynności dotyczą wyłącznie danej osoby, a jednocześnie są wymierne, nawet jeżeli schematy używane w praktyce do ich pomiaru charakteryzuje pewien stopień prawdopodobieństwa. Typowymi przykładami danych biometrycznych są odciski palców, wzorzec siatkówki, struktura twarzy, głos, ale także geometria dłoni, układ żył lub nawet pewne głęboko zakorzenione umiejętności lub inne cechy zachowania (takie jak własnoręczny podpis, uderzenie w klawisz, szczególny chód lub sposób mówienia, itp.)

Specyficzną cechą danych biometrycznych jest to, że można je uważać jednocześnie za *treść* informacji o danej osobie (te odciski palców należą do Tytusa), oraz za *łącznik* pomiędzy pewną informacją a osobą (dany przedmiot został dotknięty przez osobę mającą te odciski palców, a należą one do Tytusa; czyli przedmiot ten został dotknięty przez Tytusa). Jako takie dane biometryczne stanowią „identyfikatory". Z racji ich wyłącznej przynależności do danej osoby dane biometryczne mogą rzeczywiście być

wykorzystywane w celu ustalenie tożsamości osób. Ten specyficzny dwoisty charakter cechuje również dane DNA, które dostarczają informacji o ciele ludzkim i pozwalają na jednoznaczną identyfikację osoby.

Próbki tkanek ludzkich (jak próbki krwi) stanowią źródła, z których pochodzą dane biometryczne. Nie stanowią one natomiast danych biometrycznych same w sobie (tak jak na przykład wzorzec linii papilarnych stanowi dane biometryczne, ale sam palec nie). W związku z tym uzyskiwanie informacji z takich próbek stanowi gromadzenie danych osobowych, do których stosuje się przepisy dyrektywy. Natomiast samo gromadzenie, przechowywanie i wykorzystywanie próbek tkanek może być poddane osobnemu uregulowaniu[8].

2. DRUGI ELEMENT: „DOTYCZĄCE"

Ten element definicji jest niezwykle istotny, jako że bardzo ważne jest ustalenie, jakie związki/powiązania są istotne i w jaki sposób je rozróżnić.

Ogólnie rzecz biorąc, można uważać, że pewna informacja dotyczy osoby, jeżeli jest ona *na temat* tej osoby.

W wielu przypadkach ustalenie takiego związku jest łatwe. Na przykład dane zarejestrowane w indywidualnych aktach danej osoby w biurze kadr w jasny sposób „dotyczą" sytuacji tej osoby jako pracownika. Podobnie jest w przypadku danych o wynikach analiz medycznych pacjenta, zawartych w jego karcie, lub też w przypadku wizerunku osoby sfilmowanej w trakcie wywiadu.

W wielu innych przypadkach ustalenie, że dana informacje „dotyczą" pewnej osoby może jednak nie być tak łatwe.

W niektórych przypadkach dane przekazują przede wszystkim informacje o przedmiotach, a nie o osobach. Przedmioty te należą zazwyczaj do kogoś, podlegają wpływowi działania pewnych osób lub wywierają na nie pewien wpływ, lub też pozostają w pewnego rodzaju sąsiedztwie fizycznym lub geograficznym w stosunku do osób lub należących do nich przedmiotów. Można wtedy uznać, że informacje dotyczą tych osób lub przedmiotów jedynie pośrednio.

Przykład nr 5: wartość domu

Wartość danego domu stanowi informację o przedmiocie. Przepisy dotyczące ochrony danych nie znajdą zastosowania, jeżeli informacja taka zostanie wykorzystana wyłącznie w celu ilustracji poziomu cen nieruchomości w pewnej dzielnicy. Jednakże w pewnych okolicznościach taka informacja może również zostać uznana za dane osobowe. Dom jest dobrem należącym do pewnego właściciela i jako taki może zostać na przykład uwzględniony przy ustaleniu wysokości zobowiązań podatkowych tej osoby. W tym kontekście informację taką należy niewątpliwie uznać za dane osobowe.

Podobna analiza ma zastosowanie w przypadku, gdy dane dotyczą w pierwszym rzędzie procesów lub zdarzeń, jak na przykład informacje o funkcjonowaniu pewnej maszyny wymagającej interwencji człowieka. W pewnych okolicznościach można również uznać te informacje za „dotyczące" pewnej osoby.

[8] Patrz zalecenie nr Rec.(2006) 4 z dnia 15.3.2006 r. Komitetu Ministrów Rady Europy dla państw członkowskich w sprawie badań materiałów biologicznych ludzkiego pochodzenia.

Przykład nr 6: rejestr serwisu samochodu

Rejestr serwisu samochodu prowadzony przez mechanika lub warsztat zawiera informacje o samochodzie, przebiegu, datach przeglądów technicznych, usterkach technicznych i stanie materialnym. Informacje te są powiązane w rejestrze z numerem tablicy rejestracyjnej i numerem silnika, które z kolei mogą zostać powiązane z właścicielem. Jeżeli warsztat powiąże pojazd z jego właścicielem w celu wystawienia faktury, informacje „dotyczą" właściciela lub kierowcy. Jeżeli powiąże się informacje z mechanikiem, który pracował przy samochodzie, w celu ustalenia wydajności jego pracy, informacja ta będzie również „dotyczyła" mechanika.

Grupa robocza zwróciła już uwagę na kwestię ustalenia, kiedy dane informacje mogą zostać uznane za "dotyczące" osoby. W kontekście dyskusji nad kwestiami z zakresu ochrony danych wiążącymi się z identyfikacją radiową grupa robocza odnotowała, że „dane dotyczą osoby, jeżeli odnoszą się do tożsamości, cech lub zachowania danej osoby lub też jeśli informacje te determinują lub też wpływają na sposób traktowania lub ocenę danej osoby[9]."

Na podstawie analizy wyżej wymienionych przypadków i zgodnie z tą samą logiką można przyjąć, że aby dane można było uznać za „dotyczące" osoby, powinien występować element „**treść**", LUB element „**cel**" LUB element „**skutek**".

Element „**treść**" występuje w przypadkach, gdy – zgodnie z najoczywistszym i najbardziej rozpowszechnionym zrozumieniem słowa „dotyczyć" – informacja jest na temat pewnej osoby, niezależnie od celu, którym kieruje się administrator danych lub osoba trzecia, lub od wpływu tej informacji na osobę, której dane dotyczą. Informacja „dotyczy" osoby, jeżeli jest „na temat" tej osoby, co musi zostać ocenione w świetle wszystkich okoliczności sprawy. Przykładowo wyniki analiz medycznych w sposób ewidentny dotyczą danego pacjenta, a informacje figurujące w katalogu spółki pod nazwiskiem pewnego klienta dotyczą w sposób ewidentny tego klienta. Informacja zawarta w identyfikatorze RFID lub kodzie kreskowym umieszczonym w dokumencie tożsamości pewnej osoby (np. w przyszłych paszportach z mikroprocesorem RFID) dotyczy tej osoby.

Również element „**cel**" może sprawiać, że informacja „dotyczy" danej osoby. Można uznać, że element „cel" występuje, jeżeli dane są lub mogą być wykorzystywane, biorąc pod uwagę wszystkie okoliczności danej sprawy, w celu oceny osoby, jej traktowania w określony sposób lub też wpływania na jej status lub zachowanie.

[9] Dokument grupy roboczej nr WP 105: „dokument roboczy na temat kwestii z zakresu ochrony danych związanych w technologią RFID", przyjęty w dniu 19.1.2005 r., str. 8.

Przykład nr 7: rejestr rozmów telefonicznych

Rejestr rozmów z telefonu znajdującego się w biurze danej firmy dostarcza informacji o rozmowach przeprowadzonych z tego telefonu, który jest podłączony do pewnej linii. Informacje te można powiązać z różnymi osobami. Linia została udostępniona firmie, która jest zobowiązana w drodze umowy do uiszczania zapłaty za te rozmowy. Telefon znajduje się w godzinach pracy pod kontrolą danego pracownika i zakłada się, że to on odbył te rozmowy. Rejestr rozmów może też dostarczać informacji o osobie, do której dzwoniono. Telefonu może również użyć jakakolwiek osoba uprawniona do wejścia do lokalu podczas nieobecności pracownika (np. personel sprzątający). Informacja o używaniu telefonu może więc, w różnych celach, zostać powiązana z firmą, z pracownikiem, z personelem sprzątającym (na przykład aby sprawdzić, o której godzinie personel sprzątający opuszcza miejsce pracy, jeżeli ma on potwierdzać telefonicznie godzinę wyjścia przed zamknięciem lokalu). Należy wspomnieć, że pojęcie danych osobowych rozciąga się na połączenia wychodzące i przychodzące w zakresie, w jakim zawierają one informacje dotyczące życia prywatnego, relacji społecznych i komunikacji.

Z trzecim rodzajem informacji „dotyczących" konkretnej osoby mamy do czynienia w przypadku, gdy występuje element „**skutek**". Mimo iż nie występuje element „treść" ani „cel", dane można uważać za „dotyczące" osoby, ponieważ ich użycie będzie prawdopodobnie mieć wpływ na jej prawa i interesy, przy uwzględnieniu wszystkich okoliczności sprawy. Należy odnotować, że potencjalny skutek nie musi polegać na znacznym wpływie. Wystarczy, że pewna osoba może być traktowana odmiennie od innych osób na skutek przetwarzania takich danych.

Przykład nr 8: wpływ kontroli lokalizacji taksówek, w celu ulepszenia usługi, na kierowców

Firma taksówkowa tworzy system satelitarnego ustalania lokalizacji, który umożliwia natychmiastowe ustalenie lokalizacji wolnych taksówek. Celem przetwarzania takich danych jest polepszenie usługi i oszczędność paliwa, dzięki przypisaniu klientowi zamawiającemu taksówkę najbliższego samochodu. Mówiąc ściślej, system posługuje się danymi dotyczącymi samochodów, a nie kierowców. Celem przetwarzania danych nie jest ocena wydajności kierowców taksówek, na przykład poprzez optymalizację ich tras. Pomimo tego system pozwala na kontrolę wydajności kierowców i na sprawdzanie, czy przestrzegają oni ograniczeń prędkości, czy wybierają odpowiednie trasy, czy są za kierownicą czy poza pojazdem, itp. Może on więc mieć istotny wpływ na te osoby i w związku z tym dane można uważać za dotyczące osób fizycznych. Przetwarzanie tych danych powinno więc podlegać przepisom dotyczącym ochrony danych.

Te trzy elementy (treść, cel, skutek) stanowią warunki występujące alternatywnie, a nie łącznie. W szczególności, jeżeli występuje element „treść", wystąpienie innych elementów nie jest koniecznym warunkiem uznania informacji za dotyczącą osoby fizycznej. W związku z powyższym ta sama informacja może dotyczyć jednocześnie różnych osób, w zależności od tego, który element występuje w stosunku do każdej z nich. Ta sama informacja może dotyczyć Tytusa ze względu na element „treść" (dane są wyraźnie na temat Tytusa) ORAZ Gajusza ze względu na element „cel" (zostaną użyte w celu potraktowania Gajusza w określony sposób) ORAZ Semproniusza ze

względu na element „skutek” (dane będą prawdopodobnie mieć wpływ na prawa i interesy Semproniusza). Oznacza to, że dane nie muszą „koncentrować się” na kimś, aby można było uznać, że go dotyczą. W związku z powyższą analizą kwestię ustalenia, czy dane dotyczą określonej osoby, należy rozważać indywidualnie w przypadku każdej informacji. Dlatego też, stosując odpowiednie przepisy (np. dotyczące zakresu prawa dostępu), należy mieć na uwadze, że informacja może się odnosić do różnych osób.

Przykład nr 9: informacje zawarte w protokole z zebrania

Konieczność przeprowadzenia wyżej wymienionej analizy w przypadku każdej informacji można pokazać na przykładzie protokołu z zebrania, w którym odnotowano obecność uczestników Tytusa, Gajusza i Semproniusza; wypowiedzi Tytusa i Gajusza oraz sprawozdanie z dyskusji na pewien temat przedstawione skrótowo przez autora protokołu, Semproniusza. Za dane osobowe dotyczące Tytusa można uważać jedynie informacje o jego obecności na zebraniu danego dnia w danym miejscu oraz informacje o jego wypowiedziach. Obecność Gajusza na zebraniu, jego wypowiedzi i dyskusja na temat pewnego zagadnienia podsumowana przez Semproniusza NIE stanowią danych osobowych dotyczących Tytusa. Zasada ta obowiązuje, nawet jeżeli informacje są zawarte w tym samym dokumencie, i nawet jeżeli to Tytus doprowadził do dyskusji nad danym problemem w czasie zebrania. W związku z tym do informacji tych nie stosuje się prawo dostępu do własnych danych osobowych Tytusa. Ustalenia, czy i w jakim stopniu informacje te mogą stanowić dane osobowe Gajusza i Semproniusza, należy dokonać odrębnie, przy pomocy wyżej opisanej analizy.

3. TRZECI ELEMENT: „ZIDENTYFIKOWANEJ LUB MOŻLIWEJ DO ZIDENTYFIKOWANIA” [OSOBY FIZYCZNEJ]

Dyrektywa wymaga, aby informacja dotyczyła osoby fizycznej „zidentyfikowanej lub możliwej do zidentyfikowania”. Wiążą się z tym różne zagadnienia.

Ogólnie rzecz biorąc, można uważać osobę fizyczną za „zidentyfikowaną”, jeśli w grupie osób można ją odróżnić od wszystkich pozostałych członków grupy. Osoba fizyczna jest też „możliwa do zidentyfikowania”, jeżeli, mimo że nie została jeszcze zidentyfikowana, taka identyfikacja jest możliwa (na co wskazuje słowo „możliwa”). Ta druga możliwość jest więc w praktyce zasadniczym warunkiem przesądzającym o tym, czy informacje odpowiadają kryteriom trzeciego składnika.

Identyfikacji dokonuje się zazwyczaj dzięki poszczególnym informacjom, które można nazwać „czynnikami identyfikującymi” i które wiążą się w sposób szczególny i bliski z daną osobą. Przykładem mogą być cechy wyglądu zewnętrznego osoby, takie jak wzrost, kolor włosów, ubranie, itp., lub pewne cechy tej osoby niedostrzegalne w pierwszej chwili, takie jak zawód, stanowisko, nazwisko, itp. Dyrektywa wymienia te „czynniki identyfikujące” w definicji „danych osobowych” zawartej w art. 2, który stanowi, że tożsamość osoby fizycznej „można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość”.

Możliwa do zidentyfikowania „bezpośrednio” lub „pośrednio”

Dalsze wyjaśnienia znajdują się w komentarzu do artykułów zmienionego wniosku Komisji: „tożsamość osoby można ustalić bezpośrednio poprzez jej nazwisko lub pośrednio poprzez jej numer telefonu, numer rejestracyjny samochodu, numer ubezpieczenia społecznego, numer paszportu lub poprzez zestawienie istotnych kryteriów, które umożliwią odróżnienie tej osoby poprzez zawężenie grupy, do której ona należy (wiek, zajęcie, miejsce zamieszkania, itp.)". Ze stwierdzenia tego wynika jasno, że o tym, na ile poszczególne czynniki identyfikujące pozwalają na ostateczne ustalenie tożsamości, decydują szczególne okoliczności danej sytuacji. Bardzo pospolite nazwisko nie pozwoli na zidentyfikowanie kogoś – tzn. na wyodrębnienie go – spośród ogółu ludności danego kraju, natomiast zazwyczaj umożliwi zidentyfikowanie ucznia w klasie. Nawet drugorzędna informacja, taka jak „mężczyzna w czarnym garniturze", może pozwolić na zidentyfikowanie kogoś wśród pieszych stojących na światłach. W związku z tym ustalenie, czy osoba, której dotyczy informacja, jest zidentyfikowana czy też nie, zależy od okoliczności sprawy.

Jeśli chodzi o osobę zidentyfikowaną lub możliwą do zidentyfikowania „bezpośrednio", **nazwisko** osoby jest najoczywistszym czynnikiem identyfikującym i w praktyce pojęcie „osoby zidentyfikowanej" oznacza najczęściej odniesienie do nazwiska tej osoby.

Aby upewnić się co do tożsamości danej osoby, jej nazwisko należy czasami uzupełnić o dodatkowe dane (datę urodzenia, nazwisko rodziców, adres lub fotografię twarzy), tak aby zapobiec ewentualnemu pomyleniu jej z inną osobą noszącą to samo nazwisko. Na przykład informację o tym, że Tytus jest winien pewną sumę pieniędzy, można uważać za dotyczącą zidentyfikowanej osoby, ponieważ łączy się ona z nazwiskiem tej osoby. Nazwisko jest informacją o tym, że dana osoba używa pewnej kombinacji liter i dźwięków w celu odróżnienia się i bycia odróżnianą przez osoby, z którymi się kontaktuje. Nazwisko może też być punktem wyjścia pozwalającym na znalezienie informacji o miejscu zamieszkania lub pobytu danej osoby, a także o członkach jej rodziny (poprzez nazwisko rodowe), jak również o wielu rożnych aspektach prawnych i społecznych związanym z nazwiskiem (informacje o wykształceniu, karty pacjentów, rachunki bankowe). Może ono nawet pozwolić na zapoznanie się z wyglądem osoby, jeśli nazwisku towarzyszy zdjęcie. Wszystkie te dodatkowe informacje związane z nazwiskiem mogą pozwolić na poznanie konkretnej osoby. Poprzez czynniki identyfikujące informacje mogą zostać połączone z konkretną osobą fizyczną, która może zostać odróżniona od innych osób.

Jeśli chodzi o osobę zidentyfikowaną lub możliwą do zidentyfikowania „pośrednio", kategoria ta zwykle odnosi się do zjawiska „niepowtarzalnej kombinacji", w większym lub mniejszym wymiarze. W przypadkach gdy dostępne czynniki identyfikujące nie pozwalają *prima facie* na wyodrębnienie konkretnej osoby, osoba ta może pomimo to być „możliwa do zidentyfikowania", ponieważ informacje te, w połączeniu z innymi informacjami (którymi administrator danych dysponuje lub nie), pozwalają na odróżnienie tej osoby od innych. Tego właśnie dotyczy sformułowanie dyrektywy: „jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość". Niektóre cechy są na tyle niepowtarzalne, że pozwalają na bezproblemową identyfikację („obecny premier Hiszpanii"). Jednak również kombinacja informacji o przynależności osoby do różnych kategorii (kategoria wiekowa, pochodzenie regionalne, itp.) może być rozstrzygająca w niektórych wypadkach, zwłaszcza jeśli ma się dostęp do dodatkowych informacji. Zjawisko to było szczegółowo badane przez statystyków, zawsze pragnących uniknąć naruszenia poufności.

Przykład nr 10: częściowe informacje w prasie

Opublikowano informacje o sprawie karnej, która wzbudziła w przeszłości znaczne zainteresowanie opinii publicznej. W obecnej publikacji nie zamieszczono czynników identyfikujących podawanych zwyczajowo, między innymi nie podano nazwisk ani dat urodzenia osób mających związek ze sprawą.

Zdobycie dodatkowych informacji pozwalających na zidentyfikowanie tych osób, np. przeglądając gazety z tamtego okresu, nie jest nadmiernie trudne. Można oczekiwać, że ktoś podejmie takie działania (jak przeglądanie starych gazet), które pozwolą na dotarcie do nazwisk i innych czynników identyfikujących te osoby. W związku z tym można zasadnie uważać, że informacje podane w powyższym przykładzie stanowią „informacje o osobie możliwej do zidentyfikowania" i, jako takie, stanowią „dane osobowe".

Należy odnotować, że choć identyfikacja poprzez nazwisko jest w praktyce najczęstsza, w niektórych przypadkach nazwisko nie jest konieczne do zidentyfikowania osoby. Zdarza się tak, jeśli inne „czynniki identyfikujące" pozwalają na wyodrębnienie pewnej osoby. Na przykład pliki komputerowe rejestrujące dane osobowe nadają zazwyczaj każdej osobie niepowtarzalny identyfikator, aby uniknąć pomyłek między dwoma osobami w tym samym pliku. W Internecie narzędzia nadzorowania ruchu w sieci ułatwiają zidentyfikowanie zachowania komputera w sieci, i poprzez komputer, jego użytkownika. Odtwarza się w ten sposób osobowość danego użytkownika i przypisuje mu się pewne decyzje. Nawet nie znając nazwiska i adresu osoby, można ją zaszeregować na podstawie kryteriów społeczno-ekonomicznych, psychologicznych, filozoficznych lub innych i przypisać jej pewne decyzje, jako że punkt kontaktowy tej osoby (komputer) nie wymaga ujawnienia jej tożsamości w ścisłym sensie. Innymi słowy, możliwość zidentyfikowania danej osoby nie musi już oznaczać możliwości ustalenia jej nazwiska. Fakt ten odzwierciedla definicja danych osobowych[10].

Europejski Trybunał Sprawiedliwości wypowiedział się w tym sensie, stwierdzając, że „odniesienie na stronie internetowej do różnych osób i ich identyfikacja poprzez nazwisko lub za pomocą innych środków, na przykład poprzez podanie ich numeru telefonu lub też informacji dotyczących ich pracy lub zainteresowań stanowi przetwarzanie danych osobowych […] w rozumieniu […] dyrektywy 95/46/WE"[11].

Przykład nr 11: osoby ubiegające się o azyl

Osoby ubiegające się o azyl i ukrywające prawdziwe nazwisko w instytucji udzielającej schronienia otrzymują numer do celów administracyjnych. Numer ten ma służyć jako identyfikator pozwalający na zgromadzenie różnych informacji dotyczących pobytu osoby ubiegającej się o azyl w instytucji, a dzięki fotografii i innym parametrom biometrycznym numer ten można połączyć z daną osobą fizyczną, pozwalając w ten sposób na jej odróżnienie od innych osób ubiegających się o azyl i na

[10] Sprawozdanie na temat stosowania zasad ochrony danych w stosunku do ogólnoświatowych sieci telekomunikacyjnych, przygotowane przez Yvesa POULLETA i jego zespół dla komitetu konsultacyjnego Rady Europy ds. konwencji o ochronie osób, punkt 2.3.1, T-PD (2004) 04 wersja ostateczna.

[11] Wyrok Europejskiego Trybunału Sprawiedliwości C-101/2001 z dnia 6.11.2003 r. (Lindqvist), § 27.

przypisanie do niej różnych informacji, które będą dotyczyły osoby fizycznej „zidentyfikowanej".

Artykuł 8 ust. 7 stanowi że „państwa członkowskie określą warunki, w których może następować przetwarzanie krajowego numeru identyfikacyjnego lub innego identyfikatora ogólnego stosowania". Warto odnotować, że przepis ten, który nie zawiera żadnych konkretnych wskazówek, jakiego rodzaju warunki powinny zostać przyjęte przez państwa członkowskie, znajduje się pomimo to w artykule dotyczącym szczególnych kategorii danych. Do tego typu danych odnosi się motyw 33, który określa je jako „dane mogące ze względu na ich charakter powodować naruszenie podstawowych wolności lub prywatności". Można więc sądzić, że prawodawca odczuwał podobne obawy w stosunku do krajowych numerów identyfikacyjnych, ponieważ pozwalają one na łatwe i jednoznaczne powiązanie różnych informacji dotyczących danej osoby.

Sposoby identyfikacji

Motyw 26 dyrektywy zwraca szczególną uwagę na pojęcie „możliwa do zidentyfikowania", stwierdzając, że „w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby". Oznacza to, że czysto hipotetyczna możliwość odróżnienia osoby nie wystarcza, żeby uznać tę osobę za „możliwą do zidentyfikowania". Jeżeli, biorąc pod uwagę „wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba", prawdopodobieństwo zidentyfikowania osoby nie istnieje lub jest nieznaczne, osoba ta nie powinna zostać uznana za „możliwą do zidentyfikowania", a informacji nie należy uważać za „dane osobowe". Kryterium „wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba" powinno uwzględniać wszystkie istniejące czynniki. Jednym z czynników, chociaż nie jedynym, jest koszt identyfikacji. Należy również wziąć pod uwagę cel i sposób organizacji przetwarzania danych, spodziewane korzyści dla administratora, interesy osób, jak również ryzyko nieprawidłowości organizacyjnych (np. naruszenia obowiązku zachowania poufności) i usterek technicznych. Jest to test dynamiczny, który powinien uwzględniać stopień rozwoju technologii w momencie przetwarzania danych i możliwości jej rozwoju w okresie przetwarzania danych. Zidentyfikowanie może nie być możliwe przy pomocy wszystkich sposobów, których można użyć dzisiaj. Jeżeli dane mają być przechowywane przez miesiąc, można też przewidzieć, że identyfikacja nie będzie możliwa przez cały czas przechowywania informacji, których nie należy więc uważać za dane osobowe. Natomiast jeżeli informacje mają być przechowywane przez 10 lat, administrator powinien przewidzieć, że w dziewiątym roku przechowywania identyfikacja może stać się możliwa, w związku z czym informacje te mogą wtedy zyskać status danych osobowych. System powinien mieć być w stanie dostosować się do zmian i wdrażać we właściwym czasie odpowiednie procedury techniczne i organizacyjne.

Przykład nr 12: publikacja zdjęć rentgenowskich wraz z imieniem pacjenta

W piśmie naukowym opublikowano zdjęcie rentgenowskie pewnej kobiety, wraz z jej imieniem, które było bardzo rzadkie. Imię osoby w połączeniu z faktem, że krewni lub znajomi wiedzieli o jej chorobie, umożliwiło wielu osobom jej zidentyfikowanie, z związku z czym zdjęcie rentgenowskie należałoby uznać za dane osobowe.

Przykład nr 13: dane o badaniach farmaceutycznych

Szpitale i lekarze przekazują dane z kart pacjentów firmie farmaceutycznej w celach badawczych. Nie używa się nazwisk pacjentów, lecz przypisuje się do każdego przypadku klinicznego losowo wybrany numer, aby zapewnić ich wewnętrzną spójność i uniknąć pomylenia z danymi dotyczącymi innych pacjentów. Nazwiska pacjentów znane są jedynie poszczególnym lekarzom zobowiązanym do zachowania tajemnicy lekarskiej. Dane nie zawierają żadnych dodatkowych informacji, które po połączeniu umożliwiłyby zidentyfikowanie pacjentów. Dodatkowo podjęto wszystkie dodatkowe środki ostrożności, zarówno prawne, jak i techniczne i organizacyjne, aby zapobiec ewentualnej identyfikacji lub umożliwieniu identyfikacji osób, których dane dotyczą. W takich okolicznościach organ ds. ochrony danych może uznać, że przy przetwarzaniu danych przez firmę farmaceutyczną nie użyto sposobów, którymi można się posłużyć w celu zidentyfikowania osoby, której dane dotyczą.

Jak wspomniano powyżej, istotnym czynnikiem pozwalającym na ocenę „wszystkich sposobów, jakimi można się posłużyć" w celu zidentyfikowania osoby jest cel przetwarzania danych przez administratora. Krajowe organy ds. ochrony danych osobowych zetknęły się ze sprawami, w których administrator twierdził że przetwarza jedynie niekompletne informacje bez jakiejkolwiek wzmianki o nazwisku lub innym bezpośrednim czynniku identyfikującym i przekonywał, że dane nie powinny być uważane za dane osobowe i nie powinny podlegać przepisom dotyczącym ochrony danych osobowych. Jednak przetwarzanie takich informacji ma sens jedynie wtedy, jeżeli umożliwia zidentyfikowanie konkretnych osób i zastosowanie wobec nich określonego sposobu traktowania. W przypadkach gdy celem przetwarzania jest identyfikacja osób, można przypuszczać, że administratorzy lub inne zainteresowane osoby dysponują sposobami, „jakimi można się posłużyć" w celu zidentyfikowania osoby, której dane dotyczą. Twierdzenie, że osoby nie są możliwe do zidentyfikowania, podczas gdy celem przetwarzania danych jest właśnie ich identyfikacja, zawierałoby wewnętrzną sprzeczność. Dlatego informacje takie należy uważać za dotyczące osób możliwych do zidentyfikowania, a przetwarzanie ich powinno podlegać przepisom dotyczącym ochrony danych.

Przykład nr 14: Nadzór wideo

Dotyczy to w szczególności nadzoru wideo, w którym to kontekście administratorzy często twierdzą, że do zidentyfikowania dojdzie tylko w przypadku niewielkiej części zgromadzonych materiałów i że w związku z tym, zanim takie zidentyfikowanie nastąpi, nie przetwarza się danych osobowych. Jednakże jako że celem nadzoru wideo jest zidentyfikowanie osób występujących na obrazie wideo w każdym przypadku, gdy administrator stwierdza taką potrzebę, należy uznać cały proces za przetwarzanie danych dotyczących osób możliwych do zidentyfikowania, nawet jeżeli niektóre zarejestrowane osoby nie są możliwe do zidentyfikowania w praktyce.

Przykład nr 15: dynamiczne adresy IP

Grupa robocza uznała adresy IP za dane dotyczące osoby możliwej do zidentyfikowania. Grupa stwierdziła, że „dostawcy dostępu do Internetu i administratorzy sieci lokalnych mogą, używając sposobów, jakimi można się posłużyć, zidentyfikować użytkowników Internetu, którym przydzielili adresy IP, ponieważ systematycznie „rejestrują" oni w pliku datę, godzinę, czas trwania i dynamiczne adresy IP przydzielone użytkownikom Internetu. To samo można powiedzieć o dostawcach usług internetowych prowadzących rejestr na serwerze http. W takich

przypadkach można niewątpliwie mówić o danych osobowych w sensie art. 2 lit. a) dyrektywy…”[12].

Zwłaszcza w przypadkach, gdy przetwarzanie adresów IP ma na celu zidentyfikowanie użytkowników komputera (na przykład przez posiadaczy praw autorskich w celu ścigania użytkowników za pogwałcenie praw autorskich), administrator przewiduje, że „sposoby, jakimi można się posłużyć” w celu zidentyfikowania osoby mogą się stać dostępne, na przykład w drodze sądowej (w przeciwnym razie gromadzenie danych nie miałoby sensu), i że w związku z tym informacje te należy uważać za dane osobowe.

Szczególny przypadek stanowią niektóre rodzaje adresów IP, które w pewnych okolicznościach nie pozwalają na zidentyfikowanie użytkownika z różnych względów technicznych i organizacyjnych. Przykładem mogą być adresy IP przypisane do komputera w kawiarni internetowej, gdzie identyfikacja użytkownika nie jest wymagana. Można by twierdzić, że dane dotyczące użycia komputera X w pewnym przedziale czasowym nie pozwalają na zidentyfikowanie osoby „przy użyciu sposobów, jakimi można się posłużyć”, i że w związku z tym nie stanowią one danych osobowych. Jednakże należy odnotować, że dostawcy usług internetowych nie wiedzą najczęściej, czy dany adres IP pozwala na zidentyfikowanie, i że w związku z tym przetwarzają oni dane związane z takim adresem IP w taki sam sposób, jak informacje związane z adresami IP użytkowników zarejestrowanych i możliwych do zidentyfikowania. Dlatego też poza przypadkiem, gdy dostawca usług internetowych może stwierdzić z całkowitą pewnością, że dane dotyczą użytkowników niemożliwych do zidentyfikowania, musi on ze względów bezpieczeństwa traktować wszystkie informacje związane z adresem IP jako dane osobowe.

Przykład nr 16: szkody będące skutkiem graffiti

Pojazdy służące do przewozu osób należące do firm transportowych ponoszą regularnie szkody na skutek graffiti. Aby oszacować szkody i ułatwić dochodzenie roszczeń przeciwko ich sprawcom, firmy tworzą rejestr zawierający informacje o okolicznościach powstania szkody, jak również zdjęcia zniszczonych obiektów i „tagów” lub „podpisu” sprawcy. W momencie wpisywania informacji do rejestru sprawcy szkody nie są znani, nie wiadomo też, do kogo należy „podpis”. Może się zdarzyć, że pytania te pozostaną bez odpowiedzi. Jednakże celem przetwarzania informacji jest właśnie zidentyfikowanie osób, których informacje dotyczą, jako sprawców szkody, aby ułatwić dochodzenie roszczeń prawnych przeciwko nim. Przetwarzanie takich danych ma sens wtedy, gdy administrator danych spodziewa się, że pewnego dnia będą istniały sposoby, którymi będzie „można się posłużyć” w celu zidentyfikowania osoby. Informacje pochodzące ze zdjęć należy uważać za dotyczące osób „możliwych do zidentyfikowania”, zaś informacje figurujące w rejestrze – za „dane osobowe”; przetwarzanie takich danych powinno podlegać przepisom dotyczącym ochrony danych, które pozwalają na takie przetwarzanie pod pewnymi warunkami i z zachowaniem pewnych środków ostrożności.

Jeżeli celem przetwarzania danych nie jest zidentyfikowanie osoby, której dane dotyczą, bardzo ważną rolę odgrywają środki techniczne zapobiegające identyfikacji. Podjęcie odpowiednich, najnowocześniejszych środków technicznych i organizacyjnych w celu uniemożliwienia identyfikacji może spowodować uznanie, że

[12] WP 37 Prywatność w Internecie – zintegrowane podejście UE do problemu ochrony danych w Internecie - przyjęte w dniu 21.11.2000 r.

osoby nie są możliwe do zidentyfikowania, uwzględniając wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owych osób. Podjęcie tych środków nie wiąże się z obowiązkiem prawnym wynikającym z art. 17 dyrektywy (który stosuje się tylko, jeżeli informacje stanowią dane osobowe), lecz jest warunkiem uznania, że informacje nie stanowią danych osobowych i że przepisy dyrektywy nie mają zastosowania do ich przetwarzania.

Dane opatrzone pseudonimem

Opatrzenie pseudonimem polega na zamaskowaniu tożsamości. Celem takiej procedury jest umożliwienie gromadzenia dodatkowych danych dotyczących tej samej osoby bez potrzeby poznania jej tożsamości. Jest ona szczególnie istotna w kontekście badań naukowych i statystyki.

Opatrzenia pseudonimem można dokonać w sposób możliwy do odtworzenia poprzez użycie list zestawiających tożsamości i pseudonimy lub przez użycie dwukierunkowych algorytmów szyfrujących. Maskowania tożsamości można również dokonać w sposób uniemożliwiający ponowne zidentyfikowanie, np. w drodze szyfrowania jednokierunkowego, które pozwala zazwyczaj na stworzenie danych anonimowych.

Efektywność procedury opatrzenia pseudonimem zależy od wielu czynników (na jakim etapie się ją stosuje, w jakim stopniu jest ona zabezpieczona przed odtworzeniem, w jak dużej grupie ukryta jest dana osoba, czy możliwe jest powiązanie poszczególnych transakcji lub zapisów z tą samą osobą, itp.). Pseudonimy powinny być wybrane losowo i nieprzewidywalne. Liczba dostępnych pseudonimów powinna być na tyle duża, aby wykluczyć ewentualność ponownego wylosowania tego samego pseudonimu. Jeżeli wymagany jest wysoki stopień bezpieczeństwa, zestaw potencjalnych pseudonimów powinien być co najmniej równy zakresowi wartości bezpiecznych szyfrowych funkcji kodujących[13].

Dane opatrzone pseudonimem, które można odtworzyć, można uznać za informacje o osobach *pośrednio możliwych do zidentyfikowania*. Użycie takiego pseudonimu oznacza, że pod pewnymi z góry określonymi warunkami możliwe jest odtworzenie tożsamości osoby. W tym przypadku, choć przepisy o ochronie danych mają zastosowanie, zagrożenia związane z przetwarzaniem takich informacji o osobach pośrednio możliwych do zidentyfikowania są najczęściej niskie, co uzasadnia bardziej elastyczne stosowanie przepisów niż w przypadku przetwarzania informacji o osobach bezpośrednio możliwych do zidentyfikowania.

Dane zakodowane za pomocą klucza

Dane zakodowane za pomocą klucza są klasycznym przykładem opatrzenia pseudonimem. Informacje dotyczą osób, które są oznaczone kodem, podczas gdy klucz łączący kod ze zwyczajowymi czynnikami identyfikującymi osoby (jak nazwisko, data urodzenia, adres) jest przechowywany osobno.

Przykład nr 17: dane niezagregowane do celów statystycznych

[13] Patrz dokument roboczy „Technologie zwiększające prywatność" grupy roboczej ds. „technologii zwiększania prywatności" Komitetu ds. „aspektów technologicznych i organizacyjnych ochrony danych" niemieckiego komisarza federalnego i krajowego ds. ochrony danych (październik 1997 r.), opublikowany na stronie internetowej: http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm

Przykładem ilustrującym wagę uwzględnienia wszystkich okoliczności w celu ustalenia, czy sposobów zidentyfikowania „można użyć", może być przetwarzanie informacji osobowych przez krajowe instytuty statystyczne. W takich instytutach informacje przechowywane są na pewnym etapie w postaci niezagregowanej. Dotyczą one konkretnych osób, które są jednak oznaczone kodem, a nie nazwiskiem (np. osoba o kodzie X1234 wypija kieliszek wina co najmniej 3 razy w tygodniu). Instytut statystyczny przechowuje osobno klucz do tych kodów (listę łączącą kody z nazwiskami osób). Można uważać, że instytut statystyczny „może użyć" tego klucza, i że w związku z tym zbiór danych dotyczących osób można uważać za dane osobowe, w stosunku do których instytut powinien stosować przepisy dotyczące ochrony danych. Można sobie też wyobrazić, że lista z danymi na temat spożycia wina przez konsumentów zostanie przekazana krajowej organizacji producentów wina, aby umożliwić poparcie ich oficjalnego stanowiska danymi statystycznymi. Aby ustalić, czy ta lista informacji stanowi nadal dane osobowe, należy ocenić, czy indywidualni konsumenci wina mogą zostać zidentyfikowani, „biorąc pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba".

Jeżeli użyte kody są inne dla każdej osoby, ryzyko zidentyfikowania występuje zawsze wtedy, gdy można uzyskać dostęp do klucza używanego do szyfrowania. Dlatego też aby ocenić, czy osoby mogą być zidentyfikowane, „biorąc pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba", i czy w związku z tym informacje należy uważać za „dane osobowe", należy uwzględnić istotne czynniki takie jak ryzyko złamania kodu z zewnątrz, prawdopodobieństwo, że ktoś z organizacji – naruszając obowiązek dochowania tajemnicy zawodowej – dostarczy klucz *oraz* możliwość zidentyfikowania pośredniego. Jeżeli czynniki takie występują, zastosowanie mają przepisy dotyczące ochrony danych. Osobną kwestią jest to, czy przepisy dotyczące ochrony danych mogą uwzględniać fakt, że zagrożenia dla osób są ograniczone i stosować wobec przetwarzania danych bardziej lub mniej surowe wymagania, zgodnie z elastycznością przewidzianą przez przepisy dyrektywy.

Jeżeli zaś kody nie są niepowtarzalne, lecz ten sam numer kodu (np. „123") używany jest do oznaczenia osób w różnych miastach i danych z różnych lat (wyróżniając jedynie konkretne osoby w danym roku i w próbce z tego samego miasta), administrator lub osoba trzecia mogliby zidentyfikować konkretną osobę, wiedząc jedynie, którego roku i którego miasta dane dotyczą. Jeżeli te dodatkowe informacje zaginęły i ich odzyskanie jest mało prawdopodobne, można uważać, że informacje nie dotyczą osób możliwych do zidentyfikowania i nie podlegają przepisom dotyczącym ochrony danych.

Tego rodzaju danych używa się często w próbach klinicznych leków. Dyrektywa 2001/20 z dnia 4 kwietnia 2001 r. w sprawie wdrożenia zasady dobrej praktyki klinicznej w prowadzeniu badań klinicznych[14] ustanawia ramy prawne prowadzenia takich badań. Lekarz lub badacz („prowadzący badanie") testujący leki gromadzi informacje o wynikach klinicznych każdego pacjenta, który jest oznaczony kodem. Badacz przekazuje informacje firmom farmaceutycznym lub innym zainteresowanym osobom („sponsorom") jedynie w postaci zakodowanej, jako że interesują je jedynie informacje bio-statystyczne. Badacz przechowuje jednak oddzielnie klucz łączący kod z informacjami pozwalającymi na identyfikację poszczególnych pacjentów. Badacz jest zobowiązany do zachowania takiego klucza w celu ochrony zdrowia pacjentów na

[14] Dz.U. L 121 z 1.5.2001, str. 34.

wypadek, gdyby lekarstwa okazały się niebezpieczne, tak aby można było w razie potrzeby zidentyfikować konkretnych pacjentów i zapewnić im odpowiednie leczenie.

Problemem jest ustalenie, czy dane używane do prób klinicznych można uznać za dotyczące osób fizycznych „możliwych do zidentyfikowania" i czy w związku z tym należy stosować przepisy dotyczące ochrony danych. Zgodnie z wyżej opisaną analizą, w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby. W rozważanym przypadku identyfikacja osób (aby zapewnić im odpowiednie leczenie w razie potrzeby) jest jednym z celów przetwarzania danych zakodowanych za pomocą klucza. Firma farmaceutyczna zorganizowała system przetwarzania danych, w tym strukturę organizacyjną i relacje z badaczem, który przechowuje klucz, tak że identyfikacja osób jest nie tylko możliwością, ale wręcz koniecznością w niektórych okolicznościach. Zidentyfikowanie pacjentów jest więc jednym z celów przetwarzania danych. W przypadku tym można uznać, że takie dane zakodowane za pomocą klucza stanowią informacje dotyczące osób fizycznych możliwych do zidentyfikowania dla wszystkich stron, które mogą uczestniczyć w ewentualnej identyfikacji. Dane te powinny więc podlegać przepisom dotyczącym ochrony danych. Przetwarzanie tych samych zakodowanych danych przez innego administratora nie stanowiłoby natomiast przetwarzania danych osobowych, jeżeli w schemacie operacyjnym tego innego administratora ponowna identyfikacja byłaby wyraźnie wykluczona i jeżeli podjęto by w tym celu odpowiednie środki techniczne.

W innych dziedzinach badań lub nawet w innych segmentach tego samego projektu ponowna identyfikacja osoby, której dane dotyczą, może być wykluczona w schemacie protokołów i procedur, na przykład ponieważ nie występują żadne względy terapeutyczne. Ze względów technicznych lub innych może istnieć sposób pozwalający na ustalenie tożsamości osoby, której dotyczą dane kliniczne, ale nie przewiduje się takiej identyfikacji w jakichkolwiek okolicznościach i podjęto odpowiednie techniczne środki zapobiegawcze (np. szyfrowanie, kodowanie nieodwracalne). W tym przypadku nawet jeśli zidentyfikowanie niektórych osób, których dotyczą dane, może nastąpić pomimo wspomnianych protokołów i środków zapobiegawczych (z powodu nieprzewidzianych okoliczności, takich jak przypadkowe zestawienie ujawniających tożsamość cech osób, których dane dotyczą), nie należy uważać informacji przetwarzanych przez pierwotnego administratora za dotyczące osób zidentyfikowanych lub możliwych do zidentyfikowania, biorąc pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba. Przetwarzanie takich danych nie podlega więc przepisom dyrektywy. Natomiast w przypadku nowego administratora, który uzyskał dostęp do informacji możliwych do zidentyfikowania, będą one niewątpliwie stanowić „dane osobowe".

Schemat „bezpiecznej przystani"- NZP (najczęściej zadawane pytanie) nr 14-7

Problem danych zakodowanych za pomocą klucza w badaniach farmaceutycznych został poruszony w kontekście schematu „bezpiecznej przystani„[15]. Pytanie 14-7 brzmi następująco:

NZP 14 - Produkty farmaceutyczne i medyczne

[15] Decyzja Komisji 2000/520/WE z dnia 26.7.2000 r. – Dz.U. L 215/7 z dnia 25.8.2000.

7. P: Dane badawcze są zawsze szyfrowane na wstępie przy użyciu niepowtarzalnego kodu przez głównego badacza, tak żeby nie ujawniać tożsamości poszczególnych osób, których dane dotyczą. Spółki farmaceutyczne sponsorujące takie badania nie otrzymują klucza do szyfru. Klucz do kodu jest znany tylko badaczowi tak, że tylko on/ona może zidentyfikować obiekt badań, gdy zajdą szczególne okoliczności (np. jeżeli potrzebne jest badanie kontrolne). Czy przekazywanie z UE do Stanów Zjednoczonych danych osobowych zaszyfrowanych w ten sposób stanowi przekazanie danych osobowych podlegające zasadom „bezpiecznej przystani"?

7. O: Nie. Opisany przypadek nie stanowiłby przekazywania danych osobowych, które podlegałoby zasadom.

Grupa robocza uważa, że to stwierdzenie w schemacie „bezpiecznej przystani" nie jest niezgodne z wyżej przedstawionym rozumowaniem, według którego takie informacje uważa się za dane osobowe podlegające dyrektywie. Pytanie jest niewystarczająco precyzyjne i nie określa, komu i w jakich warunkach przekazuje się dane.
Grupa robocza uznaje, że pytanie dotyczy przypadku, gdy dane zakodowane za pomocą klucza są wysłane do odbiorcy w Stanach Zjednoczonych (na przykład firmy farmaceutycznej), który otrzymuje jedynie dane zakodowane i nie pozna nigdy tożsamości pacjentów, która znana jest i znana będzie, na wypadek gdyby potrzebne było leczenie, jedynie lekarzowi/badaczowi w UE, ale nigdy firmie w Stanach Zjednoczonych.

Dane anonimowe

„Dane anonimowe" w rozumieniu dyrektywy można zdefiniować jako wszelkie informacje dotyczące osoby fizycznej, która jest niemożliwa do zidentyfikowania przez administratora danych lub inną osobę, „biorąc pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania tej osoby". „Dane, którym nadano anonimowy charakter" są danymi anonimowymi, które wcześniej dotyczyły osoby możliwej do zidentyfikowania, lecz której zidentyfikowanie nie jest już możliwe. Motyw 26 odnosi się do tego pojęcia, stwierdzając, że „zasady ochrony danych nie mają zastosowania do danych, którym nadano anonimowy charakter w taki sposób, że podmiot danych nie będzie mógł być zidentyfikowany". Ocena, czy dane pozwalają na zidentyfikowanie osoby, czy też można je uznać za anonimowe, zależy do okoliczności. W każdym przypadku należy przeprowadzić odrębną analizę, zwracając szczególną uwagę na sposoby, jakimi można się posłużyć w celu zidentyfikowania osoby, jak wskazano w motywie 26. Dotyczy to szczególnie informacji statystycznych, w przypadku których mimo że informacje mogą być przedstawione w postaci zagregowanej, oryginalna próbka może nie być wystarczająco duża, w związku z czym inne informacje mogą umożliwić zidentyfikowanie osób.

Przykład nr 18: badania statystyczne i kombinacje rozproszonych informacji

Poza ogólnym obowiązkiem przestrzegania przepisów dotyczących ochrony danych, w celu zapewnienia anonimowości badań statystycznych statystycy podlegają szczególnemu obowiązkowi dochowania tajemnicy zawodowej, zgodnie z którym nie wolno im publikować danych innych niż anonimowe. Zobowiązuje ich to do publikacji danych statystycznych w postaci zagregowanej, które nie mogą być łatwo przypisane do zidentyfikowanej osoby.
Dotyczy to w szczególności publikacji danych pochodzących z powszechnego spisu ludności.

W każdej sytuacji należy ustalić próg, poniżej którego można uznać, że zidentyfikowanie osób jest możliwe. Jeżeli dane kryterium prowadzi do zidentyfikowania w danej grupie osób, nawet dużej (np. tylko jeden lekarz w mieście mającym 6000 mieszkańców), należy albo zupełnie odrzucić owo kryterium odróżniające, albo dodać inne kryteria, pozwalające zamaskować wyniki dotyczące danej osoby tak, aby umożliwić zachowanie tajemnicy statystycznej.
Przykład nr 19: publikacja obrazów z kamer nadzoru wideo

Sklepikarz instaluje system nadzoru wideo w swoim sklepie. Następnie publikuje on w swoim sklepie zdjęcia złodziei uchwycone dzięki systemowi nadzoru wideo. Po interwencji policji maskuje twarze złodziei, zaciemniając je. Jednakże nawet po tej operacji nadal istnieje możliwość rozpoznania osób na zdjęciach przez ich przyjaciół, krewnych lub sąsiadów, np. ponieważ ich sylwetka, fryzura lub ubrania są możliwe do rozpoznania.

4. CZWARTY ELEMENT: „OSOBY FIZYCZNEJ”

Ochrona przyznana przez przepisy dyrektywy stosuje się do osób fizycznych, to znaczy do ludzi. Prawo do ochrony danych osobowych jest w tym znaczeniu prawem uniwersalnym, a nie prawem ograniczonym do obywateli lub osób zamieszkałych w danym kraju. Motyw 2 dyrektywy zaznacza to, stwierdzając, że „systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi” i że „muszą one, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, szanować ich podstawowe prawa i wolności”.

Do pojęcia osoby fizycznej odnosi się art. 6 Powszechnej Deklaracji Praw Człowieka, zgodnie z którym „Każdy człowiek ma prawo do tego, by wszędzie uznawano jego osobowość prawną”. Ustawodawstwo państw członkowskich, zwykle w dziedzinie prawa cywilnego, określa bardziej precyzyjnie pojęcie osobowości ludzi, rozumianej jako zdolność do bycia podmiotem stosunków prawnych od urodzenia aż do śmierci. Dane osobowe stanowią więc w zasadzie dane dotyczące zidentyfikowanych lub możliwych do zidentyfikowania *żyjących osób fizycznych*. Wiąże się z tym szereg kwestii do poruszenia w niniejszej analizie.

Dane dotyczące osób nieżyjących

Danych dotyczących osób nieżyjących nie należy uważać za dane osobowe podlegające przepisom dyrektywy, jako że osoby zmarłe nie są już osobami fizycznymi w rozumieniu prawa cywilnego. Jednakże dane ich dotyczące mogą w niektórych przypadkach być chronione pośrednio.

Po pierwsze administrator danych może nie być w stanie stwierdzić, czy osoba, której dane dotyczą, nadal żyje. Nawet jeżeli ustalenie tego jest możliwe, informacje o osobach nieżyjących można przetwarzać bez rozróżnienia według takich samych procedur co informacje o osobach żyjących. Jako że administrator danych podlega obowiązkowi ochrony danych ustanowionemu przez dyrektywę w stosunku do danych na temat osób żyjących, może być mu w praktyce łatwiej przetworzyć również dane o osobach nieżyjących w sposób wymagany przez przepisy dotyczące ochrony danych, niż podzielić dane na dwie osobne kategorie.

Po drugie informacje o osobach nieżyjących mogą również dotyczyć osób żyjących. Na przykład informacja o tym, że nieżyjąca Gaja cierpiała na hemofilię wskazuje na to,

że jej syn Tytus również cierpi na tę samą chorobę, jako że związana jest ona z genem zawartym w chromosomie X. Dlatego też, jeżeli informacje stanowiące dane dotyczące osoby nieżyjącej mogą być jednocześnie uznane za dotyczące osoby żyjącej i stanowiące dane osobowe podlegające przepisom dyrektywy, dane osobowe dotyczące osoby zmarłej mogą pośrednio zostać objęte ochroną przepisów o ochronie danych.

Po trzecie, informacje o osobie zmarłej mogą podlegać szczególnej ochronie przyznanej przez przepisy inne niż ustawodawstwo dotyczące ochrony danych, ustanawiające tzw. „personalitas praeterita". Zobowiązanie do zachowania poufności personelu medycznego nie kończy się ze śmiercią pacjenta. Krajowe ustawodawstwo dotyczące prawa do ochrony wizerunku i czci może również chronić pamięć osoby nieżyjącej.

Po czwarte, nic nie stoi na przeszkodzie rozszerzeniu przez państwa członkowskie zasięgu ustawodawstwa krajowego wdrażającego przepisy dyrektywy 95/46/WE na obszary będące poza zasięgiem tej dyrektywy, o ile nie wyklucza tego żaden inny przepis prawa Wspólnoty, jak przypomniał ETS[16]. Niektórzy ustawodawcy krajowi mogą zdecydować się na rozszerzenie zakresu przepisów krajowego prawa w dziedzinie ochronie danych na aspekty dotyczące przetwarzania danych na temat osób zmarłych, jeżeli motywuje to uzasadniony interes[17].

Nienarodzone dzieci

Zakres, w jakim przepisy dotyczące ochrony danych mogą być stosowane przed urodzeniem, zależy od ogólnego stanowiska krajowego systemu prawnego na temat ochrony nienarodzonych dzieci. Biorąc głownie pod uwagę prawo do spadku, niektóre państwa członkowskie wyznają zasadę, że dziecko poczęte, ale jeszcze nie urodzone należy uważać za urodzone w zakresie, w jakim chodzi o jego korzyść (i w związku z tym może ono nabyć spadek lub przyjąć darowiznę) pod warunkiem, że się rzeczywiście urodzi. W innych państwach członkowskich przysługuje szczególna ochrona na mocy szczególnych przepisów prawnych również pod tym samym warunkiem. W celu ustalenia, czy krajowe przepisy dotyczące ochrony danych poddają ochronie również informacje o dzieciach nienarodzonych, należy uwzględnić ogólne stanowisko danego krajowego systemu prawnego, a także to, że celem przepisów dotyczących ochrony danych jest ochrona jednostek.

Inne zagadnienie wiąże się z tym, że uregulowania prawne opierają się na założeniu, iż sytuacja nienarodzonego dziecka obejmuje jedynie okres ciąży. Nie uwzględniają więc one faktu, że sytuacja ta może obecnie trwać o wiele dłużej, jak w przypadku zamrożonych embrionów. Szczególne uregulowania można także znaleźć w przepisach dotyczących technik prokreacji, w których mowa jest o wykorzystywaniu informacji medycznych lub genetycznych o embrionach.

Osoby prawne

Jako że definicja danych osobowych odnosi się do jednostek, czyli do osób fizycznych, informacje dotyczące osób prawnych w zasadzie nie podlegają dyrektywie i nie stosuje

---

16 Wyrok Europejskiego Trybunału Sprawiedliwości C-101/2001 z dnia 6.11.2003 r. (Lindqvist), § 98.

17 Protokół obrad Rady Unii Europejskiej z dnia 8.2.1995 r., dokument 4730/95: „Odnośnie do art. 2 lit. a) „ Rada i Komisja potwierdzają, że państwa członkowskie ustalają, w jakim zakresie niniejsza dyrektywa stosuje się do osób zmarłych."

się do nich przyznanej przez dyrektywę ochrony[18]. Jednakże niektóre przepisy dotyczące ochrony danych mogą w wielu przypadkach stosować się pośrednio do informacji dotyczących przedsiębiorstw lub osób prawnych.

Niektóre przepisy dyrektywy 2002/58/WE o prywatności i łączności elektronicznej dotyczą osób prawnych. Jej art. 1 stanowi, że „2. Przepisy niniejszej dyrektywy dookreślają i uzupełniają dyrektywę 95/46/WE zgodnie z celami przedstawionymi w ust. 1. Ponadto zapewniają ochronę uzasadnionych interesów abonentów będących osobami prawnymi." W związku z tym art. 12 i 13 rozszerzają zakres stosowania niektórych przepisów dotyczących spisów abonentów i komunikatów niezamówionych na osoby prawne.

Informacje o osobach prawnych można również uznać w niektórych przypadkach za „dotyczące" osób fizycznych indywidualnie, zgodnie z kryteriami przedstawionymi w niniejszym dokumencie. Może tak być, jeśli nazwa osoby prawnej pochodzi od nazwiska osoby fizycznej. Innym przypadkiem może być poczta elektroniczna firmy, używana zazwyczaj przez pewnego pracownika, lub też informacje o małym przedsiębiorstwie (z punktu widzenia prawa chodzi tu raczej o „rzecz" niż o osobę prawną), które mogą opisywać zachowanie jego właściciela. We wszystkich tych przypadkach, jeżeli kryteria „treść", „cel" lub „skutek" pozwalają na uznanie informacji o osobie prawnej lub o przedsiębiorstwie za „dotyczącą" osoby fizycznej, należy uznać je za dane osobowe i stosować przepisy dotyczące ochrony danych.

Europejski Trybunał Sprawiedliwości jasno stwierdził, że nic nie stoi na przeszkodzie rozszerzeniu przez państwa członkowskie zakresu ustawodawstwa krajowego wdrażającego przepisy dyrektywy na obszary będące poza jej zakresem, o ile nie wyklucza tego żaden inny przepis prawa Wspólnoty[19]. W związku z tym państwa członkowskie takie jak Włochy, Austria czy Luksemburg rozszerzyły zakres stosowania niektórych przepisów ustaw krajowych przyjętych zgodnie z dyrektywą (takich jak przepisy dotyczące środków bezpieczeństwa) na przetwarzania danych dotyczących osób prawnych.

Tak jak w przypadku informacji o osobach nieżyjących, podjęte przez administratora danych środki praktyczne mogą również skutkować *de facto* poddaniem danych o osobach prawnych przepisom dotyczącym ochrony danych. Jeżeli administrator danych gromadzi dane o osobach fizycznych i o osobach prawnych bez rozróżnienia w tym samym zbiorze danych, należy opracować mechanizm przetwarzania danych i system kontrolny tak, by były one zgodne z przepisami dotyczącymi ochrony danych. Administratorowi danych może być łatwiej stosować przepisy dotyczące ochrony danych do wszystkich typów informacji w zbiorach, niż ustalać, które z nich odnoszą się do osób fizycznych, a które do osób prawnych.

IV. CO DZIEJE SIĘ, JEŻELI DANE NIE ODPOWIADAJĄ DEFINICJI?

Jak to pokazuje niniejszy dokument, w różnych okolicznościach informacje można uznać za niestanowiące danych osobowych. Jest tak, kiedy danych nie można uznać za dotyczące osoby fizycznej lub jeżeli osoby nie można uznać za zidentyfikowaną lub

[18] Motyw 24 dyrektywy: „Niniejsza dyrektywa nie dotyczy ustawodawstwa dotyczącego ochrony osób prawnych w odniesieniu do przetwarzania ich danych;"

[19] Wyrok Europejskiego Trybunału Sprawiedliwości C-101/2001 z dnia 6.11.2003 r. (Lindqvist), § 98

możliwą do zidentyfikowania. Jeżeli przetwarzane informacje nie odpowiadają definicji „danych osobowych", zgodnie z art. 3 dyrektywy jej przepisy nie mają zastosowania. Nie oznacza to jednak, że w takiej sytuacji osoby fizyczne są pozbawione jakiejkolwiek ochrony. Należy wziąć pod uwagę następujące względy.

Jeżeli dyrektywa nie stosuje się, może stosować się krajowe prawo dotyczące ochrony danych. Jak stwierdzono w art. 34, dyrektywa jest skierowana do państw członkowskich. Poza jej zakresem na państwach członkowskich nie spoczywają ustanowione jej przepisami obowiązki, a zwłaszcza obowiązek wprowadzenia w życie przepisów ustawowych, wykonawczych i administracyjnych niezbędnych do spełnienia jej wymogów. Jednakże, jak objaśnił Europejski Trybunał Sprawiedliwości, nic nie stoi na przeszkodzie rozszerzeniu przez państwa członkowskie zakresu ustawodawstwa krajowego wdrażającego przepisy dyrektywy na obszary będące poza jej zakresem, o ile nie wyklucza tego żaden inny przepis prawa Wspólnoty. Można więc sobie wyobrazić, że niektóre sytuacje, w których nie mamy do czynienia z przetwarzaniem danych w rozumieniu dyrektywy, podlegają pomimo tego środkom ochronnym ustanowionym przez prawo krajowe. Może się tak zdarzyć na przykład w przypadku danych zakodowanych za pomocą klucza, niezależnie od tego, czy chodzi o dane osobowe, czy nie.

Jeżeli przepisy dotyczące ochrony danych nie stosują się, niektóre działania mogą też stanowić naruszenie art. 8 Europejskiej Konwencji Praw Człowieka, która chroni prawo do życia prywatnego i rodzinnego, w świetle daleko idącego orzecznictwa ETPC. Inne uregulowania, takie jak postanowienia o odpowiedzialności pozaumownej, prawo karne lub przepisy dotyczące przeciwdziałania dyskryminacji, mogą również chronić osoby fizyczne w przypadku, gdy nie stosuje się przepisów dotyczących ochrony danych i gdy wchodzą w grę różne uzasadnione interesy.

V. PODSUMOWANIE

W niniejszej opinii grupa robocza udziela wytycznych w sprawie sposobu rozumienia i stosowania w różnych sytuacjach pojęcia danych osobowych w dyrektywie 95/46/WE i związanym z nią prawie Wspólnoty.

Na wstępie odnotowano, że wolą europejskiego prawodawcy było przyjęcie szerokiej koncepcji danych osobowych, choć pojęcie to nie jest nieograniczone. Należy zawsze pamiętać, że celem przepisów dyrektywy jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do prywatności, w kontekście przetwarzania danych osobowych. Przepisy te należy stosować w sytuacji, gdy prawa osób fizycznych mogą być zagrożone i wymagają ochrony. Zakres przepisów dotyczących ochrony danych nie powinien być nadmiernie rozszerzany, ale należy również unikać nieuzasadnionego zawężania pojęcia danych osobowych. W dyrektywie określono zakres jego stosowania, wykluczając pewne działania, i jednocześnie pozwalając na pewną elastyczność w stosowaniu jej przepisów wobec działań, które mieszczą się w jej zakresie. Organy ochrony danych odgrywają zasadniczą rolę, decydując o odpowiedniej równowadze w stosowaniu przepisów (patrz punkt II).

Analiza grupy roboczej opiera się na czterech głównych elementach, które można odróżnić w definicji „danych osobowych": „wszelkie informacje", „dotyczące", „zidentyfikowanej lub możliwej do zidentyfikowania", „osoby fizycznej". Elementy te są ze sobą ściśle związane i wzajemnie się na sobie opierają, a połączone decydują o tym,

czy dane informacje należy uważać za „dane osobowe”. Analizę tę ilustrują przykłady z praktyki europejskich organów ochrony danych.

- Pierwszy element – „wszelkie informacje„ – wymaga szerokiej interpretacji pojęcia, niezależnie od charakteru lub treści informacji i od ich formatu technicznego. Oznacza to, że zarówno obiektywne, jak i subiektywne informacje o osobie na jakimkolwiek stanowisku można uznać za „dane osobowe”, niezależnie od nośnika technicznego, na którym są one zawarte. W opinii omówiono również dane biometryczne i rozróżnienie prawne między nimi a próbkami tkanek ludzkich, z których mogą one pochodzić (patrz punkt III.1).

- Drugi element – „dotyczące” – był dotąd często przeoczany, tymczasem odgrywa on kluczową role przy ustalaniu zakresu przedmiotowego pojęcia, szczególnie w odniesieniu do przedmiotów i nowych technologii. W opinii określono trzy alternatywne elementy – tzn. treść, cel lub skutek – pozwalające na ustalenie, czy informacje „dotyczą” osoby. Dotyczy to również informacji, które mogą mieć zdecydowany wpływ na sposób traktowania lub oceny osoby (patrz punkt III.2).

- Trzeci element – „zidentyfikowanej lub możliwej do zidentyfikowania” – dotyczy warunków pozwalających na uznanie osoby za „możliwą do zidentyfikowania”, a zwłaszcza na „sposobach, jakimi może posłużyć się” administrator danych lub inna osoba w celu zidentyfikowania owej osoby. Szczególny kontekst i okoliczności konkretnej sprawy odgrywają istotną rolę w tej analizie. Opinia odnosi się również do „danych opatrzonych pseudonimem” i do wykorzystywania „danych zakodowanych za pomocą klucza” w badaniach statystycznych lub farmaceutycznych (patrz punkt III.3).

- Czwarty element – „osoby fizycznej” – odnosi się do wymogu, aby dane osobowe dotyczyły „żyjącej osoby fizycznej”. W opinii omówiono również związki z danymi dotyczącymi osób zmarłych, nienarodzonych dzieci i osób prawnych (patrz punkt III.4).

Wreszcie, w opinii omówiono sytuację, gdy dane nie odpowiadają definicji „danych osobowych”. W przypadku takim można sięgać do różnych rozwiązań, między innymi do ustawodawstwa krajowego poza zakresem dyrektywy, pod warunkiem przestrzegania zaleceń innych aktów prawa Wspólnoty (patrz punkt IV).

Grupa robocza wzywa wszystkie zainteresowane osoby do uważnego zapoznania się z wytycznymi zamieszczonymi w niniejszej opinii i do uwzględniania ich przy wykładni i stosowaniu przepisów prawa krajowego zgodnie z dyrektywą 95/46/WE.

Członkowie grupy roboczej, głownie przedstawiciele organów nadzoru ochrony danych na poziomie krajowym, podejmują się rozwijać dalej wytyczne zamieszczone w niniejszej opinii w granicach kompetencji tych organów i zapewniać odpowiednie stosowanie prawa krajowego zgodnie z dyrektywą 95/46/WE.

Grupa robocza zamierza w razie potrzeby stosować i rozwijać wytyczne zawarte w niniejszej opinii, a także uwzględniać je w swoich dalszych pracach, w szczególności dotyczących problemów takich jak zarządzanie tożsamościami w kontekście e-administracji i e-zdrowia, jak również w kontekście identyfikacji radiowej (RFID). Odnośnie do tego ostatniego tematu, grupa robocza zamierza poddać dalszej analizie ewentualny wpływ przepisów dotyczących ochrony danych na korzystanie z technologii

RFID i zbadać, czy istnieje potrzeba wprowadzenia dodatkowych środków zapewniających w tym kontekście przestrzeganie prawa do ochrony danych i innych interesów.

Grupa robocza zwraca się do zainteresowanych osób oraz organów nadzoru o przekazywanie informacji na temat praktycznego stosowania wytycznych zamieszczonych w niniejszej opinii, wraz z przykładami mogącymi uzupełnić te wymienione w dokumencie. Grupa zamierza we właściwym czasie ponownie zająć się tym tematem, aby dalej podnosić poziom zrozumienia kluczowego pojęcia danych osobowych oraz zapewniać ujednolicone stosowanie i lepsze stosowanie dyrektywy 95/46/WE i związanego z nią prawodawstwa wspólnotowego.

W imieniu grupy roboczej

Przewodniczący
Peter SCHAAR