844/14/EN
WP 217

Opinia 6/2014 w sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy artykułu 7 dyrektywy 95/46/WE

Przyjęta w dniu 9 kwietnia 2014 r.

Niniejsza Grupa Robocza została powołana na mocy artykułu 29 Dyrektywy 95/46/WE. Jest to niezależny europejski organ doradczy w sprawach ochrony danych i prywatności. Jego zadania opisane zostały w artykule 30 Dyrektywy 95/46/WE i artykule 15 Dyrektywy 2002/58/WE.

Obsługę Sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, Biuro nr MO-59 02/013.
Strona internetowa: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Spis treści

Streszczenie

W niniejszej opinii dokonano analizy kryteriów przewidzianych w artykule 7 dyrektywy 95/46/WE, aby przetwarzanie danych było prawnie uzasadnione. Skupiając się na prawnie uzasadnionych interesach administratora, opinia przedstawia wytyczne odnośnie tego, jak stosować artykuł 7 lit. f) zgodnie z obecnymi ramami prawnymi i przedstawia zalecenia co do dalszych usprawnień.

Artykuł 7 lit. f) to ostatnia z sześciu podstaw legalnego przetwarzania danych osobowych. W rezultacie wymaga wyważenia prawnie uzasadnionych interesów administratora lub którejkolwiek ze stron trzecich, której dane są udostępniane, oraz interesów lub praw podstawowych osoby, której dane dotyczą. Wynik tego wyważenia określi, czy można opierać się na artykule 7 lit. f) jako na prawnej podstawie przetwarzania.

Grupa Robocza Art. 29 (GR Art. 29) uznaje znaczenie i przydatność kryterium z artykułu 7 lit. f), które w odpowiednich okolicznościach i z zastrzeżeniem odpowiednich zabezpieczeń może zapobiec zbytniemu opieraniu się na innych podstawach prawnych. Artykułu 7 lit. f) nie należy traktować jako ostatecznego rozwiązania w rzadkich lub nieoczekiwanych sytuacjach, w których uznaje się, że inne podstawy legalnego przetwarzania nie mają zastosowania. Jednakże nie należy go wybierać automatycznie ani niewłaściwie rozszerzać jego zastosowania na podstawie przekonania, że jest mniej ograniczający niż inne podstawy.

Właściwa ocena artykułu lit. f) to nie prosty test równowagi (wyważenia) polegający jedynie na wyważeniu dwóch łatwo policzalnych i porównywalnych wartości. Test wymaga raczej pełnego uwzględnienia szeregu czynników. Jednocześnie jest skalowalny i może być zróżnicowany, od prostego po złożony, oraz nie musi być niepotrzebnym obciążeniem. Oto czynniki, które należy uwzględnić, przeprowadzając test równowagi:

- charakter i źródło prawnie uzasadnionego interesu oraz fakt, czy przetwarzanie danych jest konieczne do realizacji prawa podstawowego, w przeciwnym razie leży w interesie publicznym lub cieszy się uznaniem przedmiotowej społeczności;

- wpływ na osobę, której dane dotyczą, oraz jej racjonalne oczekiwania na temat tego, co się stanie z jej danymi, jak również charakter danych i sposób ich przetwarzania;

- dodatkowe zabezpieczenia, które mogłyby ograniczyć nienależyty wpływ na osobę, której dane dotyczą, takie jak minimalizacja danych, technologie służące zwiększeniu ochrony prywatności; zwiększona przejrzystość, ogólne i bezwarunkowe prawo do wycofania zgody (tzw. opt-out) oraz możliwość przenoszenia danych.

Na przyszłość GR Art. 29 zaleca wprowadzenie do projektu rozporządzenia motywu dotyczącego kluczowych czynników, które należy uwzględnić, stosując test równowagi. GR Art. 29 zaleca również dodanie motywu wymagającego od administratora, gdy to właściwe, dokumentowania jego oceny w interesach o większej rozliczalności. I wreszcie GR Art. 29 opowiada się za istotnym przepisem przewidującym, że administratorzy powinni wyjaśnić osobom, których dane dotyczą, dlaczego ich zdaniem ich interesy nie będą podporządkowane interesom, prawom podstawowym i wolnościom osoby, której dane dotyczą.

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

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

uwzględniając art. 29 i 30 ust. 1 lit. a) i ust. 3 powyższej dyrektywy,

uwzględniając swój regulamin,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. Wprowadzenie

W niniejszej opinii dokonano analizy kryteriów przewidzianych w artykule 7 dyrektywy 95/46/WE [1] ('dyrektywy'), aby przetwarzanie danych było prawnie uzasadnione. W opinii skupiono się na prawnie uzasadnionych interesach administratora, zgodnie z artykułem 7 lit. f).

Kryteria wymienione w artykule 7 związane są z szerszą zasadą 'legalności' przewidzianą w artykule 6 ust. 1 lit. a), który wymaga, że dane muszą być przetwarzane 'rzetelnie i legalnie'.

Artykuł 7 wymaga, że dane osobowe powinny być przetwarzane tylko, jeżeli ma zastosowanie co najmniej jedna z sześciu podstaw prawnych wymienionych w tym artykule. W szczególności dane osobowe powinny być przetwarzane tylko (a) na podstawie jednoznacznej zgody osoby, której dane dotyczą[2]; lub – krótko mówiąc[3] - przetwarzanie jest konieczne do:

(b) realizacji umowy z osobą, której dane dotyczą;
(c) wypełnienia zobowiązania prawnego nałożonego na administratora;
(d) ochrony żywotnych interesów osoby, której dane dotyczą;
(e) realizacji zadania wykonywanego w interesie publicznym; lub
(f) prawnie uzasadnionych interesów administratora i podlega dodatkowemu testowi wyważenia z prawami i interesami osoby, której dane dotyczą.

Ta ostatnia podstawa pozwala na przetwarzanie 'konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osób, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom[4] związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które

[1] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. L 281,23.11.1995, str. 31).
[2] Patrz opinia 15/2011 Grupy Roboczej Artykułu 29 ds. Ochrony Danych w sprawie definicji zgody, przyjęta 13.07.2011 r. (WP187).
[3] Przepisy te omówiono bardziej szczegółowo na dalszym etapie.
[4] Jak wyjaśniono w części III.3.2, wydaje się, że angielska wersja dyrektywy zawiera literówkę: tekst powinien brzmieć 'interests **or** fundamental rights' ('interesom lub prawom podstawowym') zamiast 'interests **for** fundamental rights' ('interesom związanym z prawami podstawowymi').

gwarantują ochronę na podstawie art. 1 ust. 1'. Innymi słowy artykuł 7 lit. f) pozwala na przetwarzanie podlegające testowi wyważenia prawnie uzasadnionych interesów administratora – lub strony trzeciej lub osób, którym dane są ujawniane – oraz interesów i praw podstawowych osób, których dane dotyczą.[5]

Potrzeba bardziej spójnego i zharmonizowanego podejścia w całej Europie

Badania przeprowadzone przez Komisję w ramach przeglądu dyrektywy[6], jak również współpraca i wymiana poglądów między krajowymi organami ochrony danych ('OOD') wykazały brak zharmonizowanej interpretacji artykułu 7 lit. f) dyrektywy, co doprowadziło do rozbieżnego stosowania w państwach członkowskich. W szczególności, mimo że przeprowadzenie prawdziwego testu równowagi wymagane jest w kilku państwach członkowskich, artykuł 7 lit. f) jest czasami niewłaściwie postrzegany jako 'otwarte drzwi' do legitymizacji przetwarzania danych, które nie pasuje do żadnej z pozostałych podstaw.

Wynikiem braku spójnego podejścia może być brak pewności prawnej i przewidywalności, osłabienie pozycji osób, których dane dotyczą oraz nałożenie zbędnych obciążeń regulacyjnych na przedsiębiorstwa i inne organizacje działające ponad granicami. Takie niespójności doprowadziły już do sporu przed Trybunałem Sprawiedliwości Unii Europejskiej ('ETS')[7].

W związku z tym jest to szczególnie dobry moment - ponieważ prace na rzecz nowego ogólnego rozporządzenia o ochronie danych trwają – aby szósta podstawa przetwarzania (odnosząca się do 'prawnie uzasadnionych interesów') i jej relacje z innymi podstawami przetwarzania były bardziej zrozumiałe. W szczególności fakt, że w grę wchodzą prawa podstawowe osób, których dane dotyczą, pociąga za sobą to, że stosowanie wszystkich sześciu podstaw powinno – należycie i na równi – uwzględniać poszanowanie tych praw. Artykuł 7 lit. f) nie powinien stać się łatwym sposobem odejścia od przestrzegania prawa ochrony danych.

Z tego względu Grupa Robocza Artykułu 29 ds. Ochrony Danych ('Grupa Robocza'), w ramach swojego Programu prac na lata 2012-2013, postanowiła uważnie przyjrzeć się temu tematowi oraz – w celu realizacji tego Programu prac[8] - zobowiązała się do opracowania projektu niniejszej opinii.

---

[5] Odniesienie do artykułu 1 ust. 1 nie powinno być interpretowane w ten sposób, że ogranicza zakres interesów oraz praw podstawowych i wolności osoby, której dane dotyczą. Zadaniem tego odniesienia jest raczej podkreślenie ogólnego celu przepisów w zakresie ochrony danych i samej dyrektywy. W istocie artykuł 1 ust. 1 odnosi się nie tylko do ochrony prywatności, ale również do ochrony wszystkich innych 'praw i wolności osób fizycznych', a prywatność jest tylko jednym z nich.

[6] 25 stycznia 2012 r. Komisja Europejska przyjęła pakiet reformy europejskich ram prawnych ochrony danych. Pakiet obejmuje: (i) 'Komunikat' (COM(2012)9 ostateczny), (ii) wniosek dotyczący ogólnego 'rozporządzenia' ('projekt rozporządzenia') (COM(2012)11 ostateczny), oraz (iii) wniosek dotyczący 'dyrektywy' w sprawie ochrony danych w obszarze współpracy policyjnej i sądowej w sprawach karnych (COM(2012)10 ostateczny). Towarzysząca 'Ocena wpływu', zawierająca 10 załączników, przewidziana jest w dokumencie roboczym Komisji (SEC(2012)72 ostateczny). Patrz, w szczególności, badanie zatytułowane 'Ocena implementacji dyrektywy o ochronie danych', stanowiące załącznik 2 do Oceny wpływu towarzyszącej pakietowi reformy ochrony danych Komisji Europejskiej.

[7] Patrz strona 7, w nagłówku 'II.1 Krótka historia, *'Implementacja dyrektywy; wyrok ASNEF i FECEMD '*.

[8] Patrz Program prac na lata 2012-2013 Grupy Roboczej Artykułu 29 ds. Ochrony Danych przyjęty 1 lutego 2012 r. (WP190).

Wdrożenie obecnych ram prawnych i przygotowanie się na przyszłość

Sam Program prac wyraźnie określił dwa cele: 'zapewnienie właściwego wdrożenia obecnych ram prawnych', jak również 'przygotowanie się na przyszłość'.

I tak, pierwszym celem niniejszej opinii jest zapewnienie powszechnego zrozumienia obecnych ram prawnych. Cel ten idzie w ślad za wcześniejszymi opiniami w sprawie innych kluczowych przepisów dyrektywy[9]. Po drugie, w oparciu o analizę, w opinii sformułowane zostaną zalecenia, które należy uwzględnić podczas przeglądu ram prawnych ochrony danych.

Struktura opinii

Po krótkim przeglądzie historii i roli prawnie uzasadnionych interesów oraz innych podstaw przetwarzania w Rozdziale II, w Rozdziale III zostaną przeanalizowane i zinterpretowane właściwe przepisy dyrektywy, przy uwzględnieniu powszechnej podstawy wdrożonej w ustawodawstwie krajowym. Analizę tę zilustrowano praktycznymi przykładami w oparciu o doświadczenie krajowe. Analiza wspiera zalecenia przedstawione w Rozdziale IV dotyczące zarówno stosowania obecnych ram regulacyjnych, jak i w kontekście przeglądu dyrektywy.

II. Ogólne spostrzeżenia i kwestie dotyczące polityki

II.1. Krótka historia

W przeglądzie tym skupiono się na tym, jak rozwijały się koncepcje zgodności z prawem (legalności) oraz prawnych podstaw przetwarzania, w tym prawnie uzasadnionych interesów. Wyjaśniono w szczególności, jak po raz pierwszy wykorzystano potrzebę podstawy prawnej jako wymóg w kontekście wyłączeń odnoszących się do praw do ochrony prywatności, a następnie przekształcono w odrębny wymóg w kontekście ochrony danych.

Europejska Konwencja Praw Człowieka ('EKPC')

Artykuł 8 Europejskiej Konwencji Praw Człowieka, przyjętej w 1950 r., zawiera prawo do ochrony prywatności – tj. poszanowanie życia prywatnego i rodzinnego, mieszkania i korespondencji każdej osoby. Artykuł ten zakazuje ingerencji w prawo do ochrony prywatności, z wyjątkiem sytuacji, gdy jest to 'zgodne z prawem' i 'konieczne w demokratycznym społeczeństwie' w celu zaspokojenia określonych rodzajów konkretnie wskazanych, istotnych interesów publicznych.

Artykuł 8 EKPC koncentruje się na ochronie życia prywatnego i wymaga uzasadnienia każdej ingerencji w prywatność. Podejście to jest oparte na ogólnym zakazie ingerencji w prawo do prywatności i zezwala na wyjątki tylko pod ściśle określonymi warunkami. W przypadkach, w których ma miejsce 'ingerencja w prywatność', wymagana jest podstawa prawna, jak również określenie prawnie uzasadnionego celu jako warunku wstępnego oceny konieczności

[9] Np. opinia 3/2013 w sprawie ograniczenia celu, przyjęta 03.04.2013 r. (WP203), opinia 15/2011 w sprawie definicji zgody (o której mowa z przypisie 2), opinia 8/2010 w sprawie prawa właściwego, przyjęta 16.12.2010 r. (WP179) oraz opinia 1/2010 w sprawie pojęć 'administrator danych' i 'przetwarzający', przyjęta 16.02.2010 r. (WP169).

ingerencji. Podejście to wyjaśnia, że EKPC nie przewiduje listy możliwych podstaw prawnych, lecz koncentruje się na konieczności podstawy prawnej oraz na warunkach, jakie ta podstawa prawna powinna spełnić.

Konwencja 108

Konwencja 108 Rady Europy[10], otwarta do podpisu w 1981 r., wprowadza ochronę danych osobowych jako odrębne pojęcie. Ideą leżącą wówczas u podstaw nie było założenie, że przetwarzanie danych osobowych powinno być zawsze postrzegane jako '*ingerencja* w prywatność', ale raczej, że w celu *ochrony* podstawowych praw i wolności każdej osoby, a szczególnie jej prawa do prywatności przetwarzanie danych zawsze powinno spełniać określone warunki. Zatem artykuł 5 ustanawia podstawowe zasady prawa ochrony danych, w tym wymóg, aby 'dane osobowe poddawane automatycznemu przetwarzaniu były (a) zbierane i przetwarzane rzetelnie i zgodnie z prawem'. Jednakże konwencja nie przewidziała szczegółowych podstaw przetwarzania.[11]

Wytyczne OECD[12]

Wytyczne OECD, przygotowane równocześnie z Konwencją 108 i przyjęte w 1980 r., podzielają podobne idee 'zgodności z prawem', mimo że pojęcie wyrażone jest w inny sposób. Artykuł 7 Wytycznych OECD w szczególności przewiduje, że 'powinny istnieć ograniczenia co do gromadzenia danych osobowych i wszelkie tego rodzaju dane powinny być uzyskiwane w legalny i rzetelny sposób oraz, gdy to właściwie, gdy osoba, której dane dotyczą, o tym wie lub wyraziła na to zgodę'. Podstawa prawna w postaci zgody została tu wyraźnie wskazana jako możliwość, którą można wykorzystać, 'gdy to właściwe'. Będzie to wymagało uwzględnienia wchodzących w grę interesów i praw, jak również oceny tego, na ile ingerencyjny charakter ma przetwarzanie. W tym rozumieniu podejście OECD wykazuje pewne podobieństwa do – znacznie bardziej rozwiniętych – kryteriów przewidzianych w dyrektywie 95/46/WE.

Dyrektywa 95/46/WE

Gdy została przyjęta w 1995 r., dyrektywa powstała w oparciu o wcześniejsze instrumenty w zakresie ochrony danych, w tym konwencję 108 oraz wytyczne OECD. Uwzględniono również wcześniejsze doświadczenia w zakresie ochrony danych w innych państwach członkowskich.

Poza szerszym wymogiem określonym w artykule 6 ust. 1 lit. a), że dane osobowe muszą być przetwarzane 'rzetelnie i legalnie', dyrektywa dodała określony zestaw wymogów dodatkowych, jako takich jeszcze nieobecnych w ani w konwencji 108 ani w wytycznych OECD: przetwarzanie danych osobowych musi być oparte na jednej z sześciu podstaw prawnych określonych w artykule 7.

[10] Konwencja 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych.

[11] Projekt tekstu zmodernizowanej konwencji przyjęty podczas posiedzenia plenarnego Komitetu T-PD w listopadzie 2012 r. stanowi, że przetwarzanie danych może być prowadzone na podstawie zgody osoby, której dane dotyczą, lub na podstawie 'innej podstawy prawnej określonej przez prawo', podobnie jak Europejska Karta Praw Podstawowych wspomniana poniżej na stronie 8 .

[12] Wytyczne OECD dotyczące ochrony prywatności i transgranicznych przepływów danych osobowych, 11 lipca 2013 r.

Implementacja dyrektywy: wyrok ASNEF i FECEMD[13]

W sprawozdaniu Komisji zatytułowanym 'Ocena wdrożenia dyrektywy o ochronie danych'[14] podkreślono, że wdrożenie przepisów dyrektywy do prawa krajowego czasami było niezadowalające. W analizie technicznej transpozycji dyrektywy w państwach członkowskich[15] Komisja podaje dalsze szczegóły na temat implementacji artykułu 7. W analizie wyjaśniono, że podczas gdy prawa w większości Państw członkowskich przewidują sześć podstaw prawnych przy użyciu relatywnie podobnych pojęć jak te użyte w dyrektywie, elastyczność tych zasad, w rzeczywistości, doprowadziła do rozbieżnego stosowania.

Zważywszy na ten kontekst szczególnie istotne jest, że w wyroku z 24 listopada 2011 r. w sprawach *ASNEF i FECEMD* ETS uznał, że Hiszpania nie transponowała prawidłowo artykułu 7 lit. f) dyrektywy, wymagając że – przy braku zgody osoby, której dane dotyczą, - wszelkie wykorzystane istotne dane powinny pojawić się w źródłach publicznych. W wyroku uznano również, że artykuł 7 lit. f) ma bezpośredni skutek. Wyrok ogranicza margines swobody, jaki państwa członkowskie mają przy wdrażaniu artykułu 7 lit. f). W szczególności nie mogą przekroczyć cienkiej granicy między wyjaśnieniem z jednej strony a określeniem wymogów dodatkowych, które zmieniłyby zakres artykułu 7 lit. f), z drugiej strony.

Wyrok, jasno określając, że państwa członkowskie nie mogą nakładać dodatkowych jednostronnych ograniczeń i wymogów dotyczących podstaw prawnych legalnego przetwarzania danych w swoich przepisach krajowych, ma znaczące konsekwencje. Sądy krajowe i inne właściwe organy muszą interpretować przepisy krajowe w świetle tego wyroku oraz, jeżeli to konieczne, odłożyć na bok wszelkie sprzeczne krajowe przepisy i praktyki.

W świetle wyroku jest tym bardziej istotne, aby krajowe organy ochrony danych (OOD) i/lub ustawodawcy europejscy osiągnęli wyraźne i wspólne rozumienie stosowania artykułu 7 lit. f). Należy to uczynić w zrównoważony sposób, ani bez nadmiernego ograniczania ani nadmiernego rozszerzania zakresu tego przepisu.

Karta Praw Podstawowych

Od czasu wejścia w życie Traktatu z Lizbony w dniu 1 grudnia 2009 r. Europejska Karta Praw Podstawowych ('Karta') cieszy się 'taką samą wartością jak Traktaty.[16] Karta gwarantuję ochronę danych osobowych jako prawo podstawowe na mocy artykułu 8, które różni się od poszanowania życia prywatnego i rodzinnego na mocy artykułu 7. Artykuł 8 określa wymóg podstawy prawnej przetwarzania. W szczególności przewiduje, że dane osobowe muszą być przetwarzane 'na podstawie zgody osoby, której dane dotyczą, lub określonej innej podstawie prawnej przewidzianej przez prawo'.[17] Przepisy te wzmacniają zarówno znaczenie zasady zgodności z prawem, jak i potrzebę odpowiedniej podstawy prawnej przetwarzania danych osobowych.

[13] Wyrok ETS z 24.11.2011r. w sprawach C-468/10 i C-469/10 (*ASNEF i FECEMD*).
[14] Patrz załącznik 2 Oceny wpływu do pakietu reformy ochrony danych Komisji, o którym mowa w przypisie 6 powyżej.
[15] Badanie dotyczące analizy i wpływu dotyczące wdrożenia dyrektywy KE 95/46/WE w państwach członkowskich. Patrz http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.
[16] Patrz artykuł 6 ust. 1 Traktatu o Unii Europejskiej (TUE).
[17] Patrz artykuł 8 ust. 2 Karty.

Wniosek dotyczący rozporządzenia o ochronie danych

W kontekście procedury przeglądu ochrony danych zakres podstaw prawnych zgodności z prawem na mocy artykułu 7, a w szczególności zakres artykułu 7 lit. f) jest obecnie przedmiotem dyskusji.

Artykuł 6 projektu rozporządzenia wymienia podstawy zgodnego z prawem przetwarzania danych osobowych. Z kilkoma wyjątkami (które zostaną opisane dalej), sześć dostępnych zasad pozostaje w dużej mierze bez zmian w porównaniu z tymi przewidzianymi w artykule 7 dyrektywy. Komisja zaproponowała jednak, aby przedstawić dalsze wytyczne w formie aktów delegowanych.

Warto zauważyć, że w kontekście prac prowadzonych w ramach właściwej Komisji Parlamentu Europejskiego[18] podejmowano próby wyjaśnienia pojęcia prawnie uzasadnionych interesów w projekcie samego rozporządzenia. Sporządzono listę przypadków, w których prawnie uzasadnione interesy administratora danych co do zasady byłyby nadrzędne wobec prawnie uzasadnionych interesów oraz praw podstawowych i wolności osoby, której dane dotyczą, jak również drugą listę przypadków, w których byłoby odwrotnie. Listy te – określone albo w przepisach albo w motywach – przewidują istotny wkład w ocenę równowagi między prawami i interesami administratora oraz osoby, której dane dotyczą, i są uwzględnione w niniejszej opinii .[19]

II.2. Rola pojęcia

Prawnie uzasadnione interesy administratora: test równowagi jako ostateczna opcja?

Artykuł 7 lit. f) wymieniony jest jako ostatnia możliwość wśród sześciu podstaw pozwalających na zgodne z prawem przetwarzanie danych osobowych. Przepis ten wzywa do przeprowadzenia testu równowagi: to, co jest konieczne dla potrzeb wynikających z prawnie uzasadnionych interesów administratora danych (lub osoby trzeciej), musi być wyważone z interesami lub prawami podstawowymi i wolnościami osoby, której dane dotyczą. Wynik testu równowagi określa, czy można polegać na artykule 7 lit. f) jako na podstawie prawnej przetwarzania.

Elastyczny charakter tego przepisu podnosi wiele ważnych kwestii dotyczących jego dokładnego zakresu i zastosowania, co z kolei będzie analizowane w niniejszej opinii. Jednakże, co będzie wyjaśnione poniżej, niekoniecznie oznacza to, że możliwość tę należy postrzegać jako taką, którą można wykorzystać jedynie oszczędnie, aby wypełnić luki w przypadku rzadkich i nieprzewidzianych sytuacji jako ‘ostateczne rozwiązanie’ lub jako ostatnią szansę, jeżeli żadna inna podstawa nie ma zastosowania. Nie należy jej również

[18] Projekt Sprawozdania Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), z dnia 16.1.2013 r. (‘Projekt Sprawozdania Komisji LIBE‘). Patrz w szczególności: zmiany 101 i 102. Patrz również: zmiany przyjęte przez Komisję 21.10.2013 r. w jej ostatecznym sprawozdaniu ('Ostateczne Sprawozdanie Komisji LIBE ').

[19] Patrz część III.3.1, w szczególności tirety na stronach 24-25 zawierające niewyczerpującą listę niektórych najpowszechniejszych kontekstów, w których może powstać kwestia prawnie uzasadnionego interesu na mocy artykułu 7 lit. f.

traktować jako preferowanej możliwości, a jej wykorzystania jako niepotrzebnie rozszerzonego, ponieważ uważana byłaby za mniej ograniczającą niż inne podstawy.

Zamiast tego równie dobrze może być tak, że artykuł 7 lit. f) ma swój własny naturalny obszar odniesienia i że może odgrywać bardzo pożyteczną rolę jako podstawa zgodnego z prawem przetwarzania, pod warunkiem spełnienia szeregu kluczowych warunków.

Odpowiednie wykorzystanie artykułu 7 lit. f), we właściwych okolicznościach i z zastrzeżeniem odpowiednich gwarancji, może również pomóc zapobiec nadużywaniu innych podstaw prawnych i zbytniemu poleganiu na nich.

Pierwsze pięć podstaw z artykułu 7 opiera się na zgodzie osoby, której dane dotyczą, postanowieniach umownych, zobowiązaniu prawnym lub innej konkretnie określonej przesłance jako podstawie legalności. Gdy przetwarzanie jest oparte na jednej z tych pięciu podstaw, uznaje się je *a priori* za legalne i w związku z tym za podlegające jedynie zgodności z innymi właściwymi przepisami prawa. Innymi słowy istnieje założenie, że równowaga między różnymi wchodzącymi w grę prawami i interesami - w tym administratora i osoby, której dane dotyczą – jest zapewniona, zakładając oczywiście, że zapewniona jest zgodność z wszystkimi innymi przepisami prawa ochrony danych. Z drugiej strony artykuł 7 lit. f) wymaga *specjalnego* testu w przypadkach, które nie wpisują się w scenariusze z góry określone w podstawach (a) - (e). Zapewnia, że, poza tymi scenariuszami, wszelkie przetwarzanie musi spełniać wymóg testu równowagi, przy należytym uwzględnieniu interesów i praw podstawowych osoby, której dane dotyczą.

Test ten może doprowadzić w niektórych przypadkach do wniosku, że równowaga przechyla się na korzyść interesów i praw podstawowych osób, których dane dotyczą, oraz że w konsekwencji przetwarzanie nie może mieć miejsca. Z drugiej strony odpowiednia ocena równowagi na mocy artykułu 7 lit. f), często z możliwością wycofania zgody na przetwarzanie (tzw. opt-out), może w innych przypadkach być ważnym rozwiązaniem alternatywnym wobec nieodpowiedniego wykorzystania na przykład podstawy ‘zgody’ lub ‘konieczności realizacji umowy’. Rozpatrywany w ten sposób, artykuł 7 lit. f) stanowi uzupełniające gwarancje – które wymagają odpowiednich środków – w porównaniu z innymi wcześniej określonymi podstawami. Zatem nie powinien być uwzględniany jako ‘najsłabsze ogniwo’ lub otwarte drzwi do legitymizacji wszystkich operacji przetwarzania danych, które nie podlegają żadnej z innych podstaw prawnych.

Grupa Robocza powtarza, że przy interpretacji zakresu artykułu 7 lit. f) dąży do zrównoważonego podejścia, które zapewnia niezbędną elastyczność administratorom danych w sytuacjach, gdy nie ma niewłaściwego wpływu na osoby, których dane dotyczą, zapewniając jednocześnie osobom, których dane dotyczą wystarczającą pewność prawną i gwarancje, że ten elastyczny przepis nie będzie nadużywany.

II.3. Koncepcje powiązane

Związek artykułu 7 lit. f) z innymi podstawami legalności

Artykuł 7 wymienia najpierw zgodę, a potem inne podstawy legalności, w tym umowy i zobowiązania prawne, stopniowo przechodząc do testu prawnie uzasadnionego interesu, który wymieniony jest jako ostatni wśród sześciu dostępnych podstaw. Porządek, w jakim wymienione są podstawy prawne w artykule 7, interpretowano czasami jako wskazanie określonego znaczenia różnych podstaw. Jednakże, jak już podkreślono w opinii Grupy Roboczej w sprawie pojęcia zgody[20], tekst dyrektywy nie wprowadza rozróżnienia prawnego między sześcioma podstawami i nie sugeruje, że istnieje wśród nich hierarchia. Brak jest wskazania, że artykuł 7 lit. f) powinien być stosowany tylko w wyjątkowych przypadkach, a tekst nie sugeruje również w inny sposób, że określony porządek sześciu podstaw będzie miał jakiś prawnie wiążący skutek. Jednocześnie dokładne znaczenie artykułu 7 lit. f) oraz jego związek z innymi podstawami legalności od dawna były niejasne.

W związku z powyższym oraz uwzględniając różnice historyczne i kulturowe oraz elastyczny język dyrektywy, opracowano różne podejścia: niektóre państwa członkowskie miały tendencję do postrzegania artykułu 7 lit. f) jako najmniej preferowanej podstawy, która ma zapełnić luki jedynie w kilku wyjątkowych przypadkach, gdy nie miałaby lub nie mogłaby mieć zastosowania żadna z pięciu pozostałych podstaw.[21] Inne państwa członkowskie, dla odmiany, postrzegają tę podstawę tylko jako jedną z sześciu możliwości, i nie jest ona ani ważniejsza ani mniej ważna niż inne możliwości, oraz może mieć zastosowanie w dużej ilości różnorodnych sytuacji, pod warunkiem spełnienia niezbędnych warunków.

Uwzględniając te różnice oraz w świetle orzeczenia ASNEF i FECEMED, ważne jest wyjaśnienie związku podstawy dotyczącej 'prawnie uzasadnionych interesów' z innymi podstawami legalności, np. w odniesieniu do zgody, umów, zadań realizowanych w interesie publicznym, jak również w odniesieniu do prawa osoby, której dane dotyczą, do wyrażenia sprzeciwu. Może to pomóc lepiej zdefiniować rolę i funkcję podstawy dotyczącej prawnie uzasadnionych interesów oraz w ten sposób może przyczynić się do pewności prawnej.

Należy również zauważyć, że podstawa dotycząca prawnie uzasadnionych interesów, wraz z innymi podstawami, oprócz zgody, wymaga przeprowadzenia testu 'konieczności'. Ogranicza to ściśle kontekst, w jakim każda z nich może mieć zastosowanie. Europejski Trybunał Sprawiedliwości uznał, że 'konieczność' to pojęcie, które ma swoje własne niezależne

[20] Patrz przypis 2 powyżej.

[21] Należy również zauważyć, że w projekcie sprawozdania Komisji LIBE zaproponowano oddzielenie artykułu 7 lit. f od pozostałych podstaw prawnych, jak również zaproponowano dodatkowe wymogi w przypadku, gdy polega się na tej podstawie prawnej, w tym większą przejrzystość i solidniejszą rozliczalność, co zostanie pokazane później.

znaczenie w prawie wspólnotowym[22]. Europejski Trybunał Praw Człowieka również przestawił przydatne wytyczne.[23]

Ponadto, posiadanie odpowiedniej podstawy prawnej nie zwalnia administratora danych z jego zobowiązań na mocy artykułu 6 w odniesieniu do rzetelności, legalności, konieczności i proporcjonalności, jak również jakości danych. Na przykład, nawet jeżeli przetwarzanie danych oparte jest na podstawie dotyczącej prawnie uzasadnionych interesów lub realizacji umowy, nie pozwoli to na gromadzenie danych, które są nadmierne w odniesieniu do określonego celu.

Prawnie uzasadnione interesy oraz inne podstawy prawne z artykułu 7 to alternatywne podstawy i w związku z tym wystarczy, jeżeli będzie miała zastosowanie tylko jedna z nich. Jednakże pojawiają się łącznie nie tylko z wymogami artykułu 6, ale również z wszystkimi innymi zasadami i wymogami ochrony danych, które mogą mieć zastosowanie.

Inne testy równowagi

Artykuł 7 lit. f) to nie jedyny test równowagi przewidziany w dyrektywie. Na przykład artykuł 9 wzywa do wyważenia prawa do ochrony danych osobowych oraz wolności wypowiedzi. Artykuł ten pozwala, aby państwa członkowskie przewidziały konieczne wyłączenia i odstępstwa w przypadku przetwarzania danych osobowych ‘prowadzonego wyłącznie w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego’, ‘gdy jest to konieczne dla pogodzenia prawa do zachowania prywatności z przepisami dotyczącymi wolności wypowiedzi'.

Ponadto wiele innych przepisów dyrektywy również wymaga analizy konkretnych przypadków, wyważenia wchodzących w grę interesów i praw oraz elastycznej wieloelementowej oceny. Chodzi tu m.in. o przepisy dotyczące konieczności, proporcjonalności oraz ograniczenia celu, wyłączenia z artykułu 13, oraz badania naukowe.

Rzeczywiście wydaje się, że dyrektywę opracowano tak, aby zostawić pole do interpretacji i wyważenia interesów. Miało to oczywiście, przynajmniej po części, zostawić dalsze pole państwom członkowskim do wdrożenia do prawa krajowego. Jednakże, oprócz tego, z samego charakteru prawa do ochrony danych osobowych oraz prawa do prywatności wynika również potrzeba określonej elastyczności. W istocie oba te prawa, wraz z większością innych praw podstawowych (ale nie ze wszystkimi), uznawana jest za kwalifikowane prawa człowieka.[24] Tego rodzaju prawa należy zawsze interpretować w kontekście. Z zastrzeżeniem

[22] Wyrok Europejskiego Trybunału Sprawiedliwości z 16 grudnia 2008 r. w sprawie C-524/06 (Heinz Huber v Bundesrepublik Deutschland), ustęp 52: W rezultacie zważywszy na cel polegający na zapewnieniu jednolitego poziomu ochrony we wszystkich państwach członkowskich, pojęcie konieczności w rozumieniu art. 7 lit. e) dyrektywy 95/46, które służy precyzyjnemu wyodrębnieniu sytuacji, w których przetwarzanie danych osobowych jest dozwolone, nie może mieć różnego zakresu w poszczególnych państwach członkowskich. Mamy tutaj zatem do czynienia z autonomicznym pojęciem prawa wspólnotowego, którego wykładnia winna w pełni odpowiadać celowi tej dyrektywy sformułowanemu w jej art. 1 ust. 1.'

[23] Wyrok Europejskiego Trybunału Praw Człowieka w sprawie Silver & Others v United Kingdom z 25 marca 1983 r., ustęp 97, w którym omówiono pojęcie 'konieczny w demokratycznym społeczeństwie': ‘przymiotnik "konieczny" nie jest synonimem przymiotnika „niezbędny”, nie charakteryzuje się również taką elastycznością jak wyrażenia takie jak „dopuszczalny”, „zwykły”, „przydatny”, „racjonalny” czy też „pożądany" ….'

[24] Istnieje tylko kilka praw człowieka, których nie można wyważyć w odniesieniu do praw innych lub interesów szerszej społeczności. Znane są one jako prawa absolutne. Praw tych nigdy nie można ograniczyć, niezależnie

odpowiednich gwarancji, mogą być wyważone w odniesieniu do praw innych. W niektórych sytuacjach – i również z zastrzeżeniem odpowiednich gwarancji – można je również ograniczyć na podstawie interesu publicznego.

II.4. Kontekst i konsekwencje strategiczne

Zapewnienie legalności, ale również elastyczności: sposoby specyfikacji artykułu 7 lit. f)

Obecne brzmienie artykułu 7 lit. f) dyrektywy ma charakter elastyczny. Oznacza to, że można na nim polegać w szeregu różnych sytuacji, o ile zostaną spełnione jego wymogi, w tym test równowagi. Jednakże taka elastyczność może mieć negatywne skutki. Aby zapobiec sytuacji, w której doprowadzi się do niespójnego stosowania krajowego lub braku pewności prawnej, istotną rolę odgrywać będą dalsze wytyczne.

Komisja przewiduje takie wytyczne w projekcie rozporządzenia w postaci aktów delegowanych. Do innych możliwości należy zapewnienie wyjaśnień i szczegółowych przepisów w samym tekście rozporządzenia[25] oraz powierzenie Europejskiej Radzie Ochrony Danych ('EROD') zadania zapewnienia dalszych wytycznych w tym obszarze.

Każda z tych możliwości z kolei ma zalety i wady. Jeżeli ocena dokonywana byłaby dla konkretnych przypadków bez dalszych wytycznych, wiązałoby się z tym ryzyko niespójnego stosowania i braku przewidywalności, co miało miejsce w przeszłości.

Z drugiej strony przewidzenie w tekście samego projektu rozporządzenia szczegółowych, wyczerpujących list sytuacji, w których prawnie uzasadnione interesy administratora co do zasady są nadrzędne wobec praw podstawowych osoby, której dane dotyczą lub vice versa, mogłoby wiązać się z ryzykiem, że przepisy te będą wprowadzały w błąd i/lub będą niepotrzebnie normatywne.

Niemniej podejścia te mogą być inspiracją do zrównoważonego rozwiązania, przewidując więcej szczegółów w samym projekcie rozporządzenia oraz dalsze wytyczne w aktach delegowanych lub w wytycznych EROD.[26]

Analiza w rozdziale III ma na celu stworzenie podstaw merytorycznych do znalezienia takiego podejścia, ani zbyt ogólnego, aby nie było bez znaczenia, ani zbyt szczegółowego, aby nie było zbyt radykalne.

---

od okoliczności – nawet w stanie wojny lub w stanie wyjątkowym. Jednym z przykładów jest prawo do tego, aby nie być poddawanym torturom ani nie być traktowanym w nieludzki lub poniżający sposób. Nigdy nie jest dopuszczalne torturowanie lub traktowanie kogoś w nieludzki lub poniżający sposób, niezależnie od okoliczności. Przykładami praw niebędących prawami absolutnymi są prawo do poszanowania życia prywatnego i rodzinnego, prawo do wolności wypowiedzi oraz prawo do wolności myśli, sumienia i religii.

[25] Patrz część II.1 Krótka historia, *'Projekt rozporządzenia o ochronie danych'* na str. 8-9.

[26] Jeżeli chodzi o akty delegowane i wytyczne EROD, w opinii Grupy Roboczej 08/2012 przedstawiającej dalsze uwagi dotyczące dyskusji na temat reformy ochrony danych, przyjętej 05.10.2012 r. (WP199), silnie opowiedziano się za tymi ostatnimi (patrz str. 13-14).

III. Analiza przepisów

III.1. Przegląd artykułu 7

Zgodnie z wymogami artykułu 7 dane osobowe mogą być przetwarzane tylko wówczas, gdy ma zastosowanie co najmniej jedna z sześciu podstaw prawnych wymienionych w tym artykule. Przed przeanalizowaniem każdej z tych podstaw, w niniejszym rozdziale III.1 przedstawiono przegląd artykułu 7 oraz jego związek z artykułem 8 dotyczącym szczególnych kategorii danych.

III.1.1. Zgoda lub 'konieczne dla...'

Można dokonać rozróżnienia między przypadkiem, gdy dane osobowe są przetwarzane na podstawie jednoznacznej zgody osoby, której dane dotyczą (artykuł 7 lit. a), a pozostałymi pięcioma przypadkami (artykuł 7 lit. b)-f)). Te pięć przypadków – krótko mówiąc – opisuje scenariusze, w których przetwarzanie może być konieczne w określonym kontekście, takim jak realizacja umowy z osobą, której dane dotyczą, wypełnienie zobowiązania prawnego nałożonego na administratora, etc.

W pierwszym przypadku, przewidzianym w artykule 7 lit. a), to same osoby, których dane dotyczą, zezwalają na przetwarzanie swoich danych osobowych. Do nich należy decyzja, czy pozwolą na przetwarzanie ich danych. Jednocześnie zgoda nie wyklucza potrzeby przestrzegania zasad przewidzianych w artykule 6[27]. Ponadto zgoda nadal musi spełniać określone niezbędne warunki, aby była legalna, jak wyjaśniono w opinii 15/2011 Grupy Roboczej[28]. W związku z tym, że przetwarzanie danych użytkownika zależy całkowicie od jego uznania, nacisk kładzie się na ważność i zakres zgody osoby, której dane dotyczą.

Innymi słowy, pierwsza podstawa, z artykułu 7 lit. a), koncentruje się na samostanowieniu osoby, której dane dotyczą, jako podstawie legalności. Wszystkie pozostałe podstawy, dla odmiany, pozwalają na przetwarzanie – z zastrzeżeniem gwarancji i środków – w sytuacjach, gdy, niezależnie od zgody, właściwe i konieczne jest przetwarzanie danych w określonym kontekście w celu osiągnięcia określonego prawnie uzasadnionego interesu.

Każda z liter (b), (c), (d) oraz (e) określa kryterium legalności przetwarzania:

(b) realizacja umowy z osobą, której dane dotyczą;
(c) wykonanie zobowiązania prawnego nałożonego na administratora;
(d) ochrona żywotnych interesów osoby, której dane dotyczą;
(e) realizacja zadania wykonywanego w interesie publicznym.

[27] Wyrok duńskiego Sądu Najwyższego z dnia 9 września 2011 r. w sprawie ECLI:NL:HR:2011:BQ8097, §3.3(e) w odniesieniu do zasady proporcjonalności. Patrz także strona 7 opinii Grupy Roboczej 15/2011, cytowana w przypisie 2 powyżej: '... Ponadto uzyskanie zgody nie zwalnia administratora danych z obowiązków na mocy art. 6 związanych z rzetelnością, koniecznością i proporcjonalnością, jak też jakością danych. Na przykład nawet jeżeli użytkownik wyraził zgodę na przetwarzanie danych osobowych, nie czyni to legalnym gromadzenia danych nadmiernych w stosunku do określonego celu.'

[28] Patrz strony 11-25 opinii 15/2011, o której mowa w przypisie 2 powyżej.

Treść lit. (f) ma mniej konkretny charakter i odnosi się, bardziej ogólnie, do (wszelkiego rodzaju) prawnie uzasadnionego interesu administratora (w każdym kontekście). Jednak dla tego ogólnego przepisu przewidziano specjalnie podleganie dodatkowemu testowi równowagi, który ma na celu ochronę interesów i praw osób, których danych dotyczą, co zostanie wykazane w części III.2 poniżej.

Ocena, czy spełniono kryteria określone w artykule 7 lit. a) - f), jest we wszystkich przypadkach początkowo dokonywana przez administratora danych, podlegając prawu właściwemu i wytycznym dotyczącym tego, jak prawo powinno być stosowane. W drugim przypadku legalność przetwarzania może podlegać dalszej ocenie i może ewentualnie być podważona przez osoby, których dane dotyczą, innych interesariuszy, organy ochrony danych, oraz ostatecznie może zdecydować o niej sąd.

Na koniec tego krótkiego przeglądu należy wspomnieć, że, co zostanie omówione w części III.3.6, co najmniej w przypadkach, o których mowa w literach e) oraz f), osoba, której dane dotyczą, może realizować prawo wyrażenia sprzeciwu, jak przewidziano w artykule 14[29]. Przyczyni się to do nowej oceny przedmiotowych interesów lub w przypadku marketingu bezpośredniego (artykuł 14 lit. b)) - wymagać będzie od administratora zaprzestania przetwarzania danych osobowych bez dalszej oceny.

III.1.2. Związek z artykułem 8

Artykuł 8 dyrektywy dalej reguluje przetwarzanie określonych kategorii danych osobowych. Ma zastosowanie konkretnie do danych ‘ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia seksualnego’ (artykuł 8 ust. 1), oraz do danych ‘dotyczących przestępstw lub wyroków skazujących’(artykuł 8 ust. 5).

Przetwarzanie takich danych jest w zasadzie zabronione, z zastrzeżeniem określonych wyłączeń. Artykuł 8 ust. 2 przewiduje szereg wyłączeń od tego zakazu, w literach a) - e). Artykuł 8 ust. 3 oraz 4 przewiduje dalsze wyłączenia. Niektóre z tych przepisów są podobne - ale nie identyczne – do przepisów przewidzianych w artykule 7 lit. a) - (f).

Określone warunki artykułu 8, jak również fakt, że niektóre podstawy wymienione w artykule 7 przypominają warunki określone w artykule 8, podnoszą pytanie o związek między tymi dwoma przepisami.

Jeżeli artykuł 8 jest opracowany jako *lex specialis*, należy rozważyć, czy wyklucza on zastosowanie artykułu 7 całkowicie. Jeżeli tak, oznaczałoby to, że szczególne kategorie danych osobowych mogą być przetwarzane bez zapewnienia zgodności z artykułem 7, pod warunkiem że ma zastosowanie jedno z wyłączeń wskazanych w artykule 8. Jednak możliwe jest również, że związek jest bardziej złożony i należy stosować artykuły 7 i 8 łącznie.[30]

---

[29] Zgodnie z artykułem 14 lit. a) prawo to ma zastosowanie ‘z zastrzeżeniem odmiennych postanowień ustawodawstwa krajowego'. Na przykład w Szwecji prawo krajowe nie pozwala na możliwość wyrażenia sprzeciwu wobec przetwarzania, które oparte jest na artykule 7 lit. e).

[30] Jako że artykuł 8 jest ustanowiony jako *zakaz z wyłączeniami,* wyłączenia te można postrzegać jako wymogi, które jedynie ograniczają zakres zakazu, ale nie stanowią, same w sobie, wystarczającej podstawy prawnej

W każdym razie jest jasne, że celem polityki jest zapewnienie dodatkowej ochrony szczególnym kategoriom danych. W związku z tym ostateczny wynik analizy powinien być równie jasny: zastosowanie artykułu 8, czy to samego czy łącznie z artykułem 7, ma na celu zapewnienie wyższego poziomu ochrony szczególnych kategorii danych.

W praktyce, podczas gdy w niektórych przypadkach artykuł 8 niesie ze sobą bardziej restrykcyjne wymogi – takie jak 'wyraźna' zgoda przewidziana w artykule 8 ust. 2 lit. a), w porównaniu z 'jednoznaczną zgodą' przewidzianą w artykułu 7 – nie odnosi się to do wszystkich przepisów. Wydaje się, że niektóre wyłączenia przewidziane w artykule 8 nie są równoznaczne z lub bardziej restrykcyjne niż podstawy wymienione w artykule 7. Niewłaściwa byłaby konkluzja na przykład, że fakt, iż ktoś ewidentnie upublicznił szczególne kategorii danych na mocy artykułu 8 ust. 2 lit. e), byłby – zawsze i sam w sobie – wystarczającym warunkiem do pozwolenia na wszelkiego rodzaju przetwarzanie danych, bez oceny równowagi interesów oraz praw wchodzących w grę, jak wymaga artykuł 7 lit. f)[31].

W niektórych sytuacjach fakt, że administratorem danych jest partia polityczna, również znosi zakaz przetwarzania szczególnych kategorii danych na mocy artykułu 8 ust. 2 lit. d). Jednakże nie oznacza to, że każde przetwarzanie podlegające zakresowi tego przepisu jest koniecznie zgodne z prawem. Należy to ocenić odrębnie i może być tak, że administrator będzie musiał wykazać na przykład, że przetwarzanie danych jest konieczne dla realizacji umowy (artykuł 7 lit. b)), lub że nadrzędny jest jego prawnie uzasadniony interes przewidziany w artykule 7 lit. f). W tym ostatnim przypadku musi być przeprowadzony test równowagi na mocy artykułu 7 lit. f), po dokonaniu oceny, że administrator danych spełnia wymogi artykułu 8.

W podobny sposób sam fakt, że 'przetwarzanie wymagane jest do celów medycyny prewencyjnej, diagnostyki medycznej, świadczenia opieki lub leczenia, lub też zarządzania opieką zdrowotną' i dane te są przetwarzane z obowiązkiem zachowania poufności – jak wskazano w artykule 8 ust. 3 – oznacza, że takie przetwarzanie danych szczególnie chronionych jest *zwolnione z zakazu* z artykułu 8 ust. 1. Jednak niekoniecznie jest to wystarczające do tego, aby zapewnić również legalność zgodnie z artykułem 7, i będzie wymagało podstawy prawnej, takiej jak umowa z pacjentem na mocy artykułu 7 lit. b), zobowiązanie prawne na mocy artykułu 7 lit. c), realizacja zadania wykonywanego w interesie publicznym na mocy artykułu 7 lit. e) czy też ocena na mocy artykułu 7 lit. f).

Podsumowując, Grupa Robocza uważa, że analizy należy dokonywać dla konkretnych przypadków niezależnie od tego, czy to artykuł 8 sam w sobie przewiduje bardziej restrykcyjne i wystarczające warunki[32], czy też wymagane jest łączne stosowanie zarówno

---

przetwarzania. W tym brzmieniu zastosowanie wyłączeń z artykułu 8 nie wyklucza zastosowania wymogów przewidzianych w artykule 7 i oba, gdy to właściwe, musza być stosowane łącznie.

[31] Ponadto artykułu 8 ust. 2 lit. e) nie należy interpretować *a contrario* jako oznaczający, że gdy dane są upubliczniane przez osobę, której dane dotyczą, nie są danymi szczególnie chronionymi, mogą być przetwarzane bez dodatkowego warunku. Publicznie dostępne dane są nadal danymi osobowymi podlegającymi wymogom ochrony danych, w tym zgodności z artykułem 7, niezależnie od tego, czy są danymi szczególnie chronionymi czy nie.

[32] Patrz analiza dokonana w opinii Grupy Roboczej nt. WADA, punkt 3.3, który bierze pod uwagę zarówno artykuł 7, jak i 8 dyrektywy: Druga opinia 4/2009 dotycząca międzynarodowego standardu ochrony prywatności i danych osobowych Światowej Agencji Antydopingowej (WADA), odnośnych postanowień kodeksu WADA oraz innych kwestii dotyczących prywatności w kontekście walki WADA i innych (krajowych) organizacji antydopingowych z dopingiem w sporcie, przyjęta 06.04.2009 r. (WP162).

artykułu 8, jak i 7, w celu zapewnienia pełnej ochrony osoby, której dane dotyczą. W żadnym przypadku wynik analizy nie powinien prowadzić do niższej ochrony szczególnych kategorii danych[33].

Oznacza to również, że administrator przetwarzający szczególne kategorie danych nigdy nie może odwoływać się *jedynie* do podstawy prawnej z artykułu 7 w celu legitymizacji przetwarzania danych. Gdy to właściwe, artykuł 7 nie będzie miał charakteru *nadrzędnego,* ale zawsze będzie miał zastosowanie *łącznie* z artykułem 8 w celu zapewnienia, że wszystkie istotne gwarancje i środki będą przestrzegane. Będzie to tym bardziej istotne w przypadku, gdy państwo członkowskie postanowi dodać dodatkowe wyłączenia do tych z artykułu 8, jak przewidziano w artykule 8 ust. 4.

III.2. Artykuł 7 lit. a)-e)

Niniejsza część III.2 przedstawia krótki przegląd każdej z podstaw prawnych przewidzianych w artykule 7 lit. a) - (e) dyrektywy, zanim opinia skoncentruje się, w części III.3, na artykule 7 lit. f). Analiza ta zwróci również uwagę na najbardziej powszechne obszary wzajemnego oddziaływania tych podstaw prawnych, na przykład dotyczących ‘umowy’, ‘zobowiązania prawnego’ oraz ‘prawnie uzasadnionego interesu’, w zależności od konkretnego kontekstu oraz stanu faktycznego.

III.2.1. Zgoda

Zgoda jako podstawa prawna była przedmiotem analizy w opinii Grupy Roboczej 15/2011 w sprawie definicji zgody. Główne ustalenia poczynione w opinii dotyczą tego, że zgoda jest jedną z kilku podstaw prawnych przetwarzania danych osobowych, a nie główną podstawą. Odgrywa ważną role, ale nie wyklucza możliwości, w zależności od kontekstu, że inne podstawy prawne będą bardziej właściwe albo z perspektywy administratora albo osoby, której dane dotyczą. Jeżeli jest wykorzystywana odpowiednio, zgoda jest narzędziem dającym osobie, której dane dotyczą, kontrolę nad przetwarzaniem jej danych. Jeżeli jest nieodpowiednio wykorzystywana, kontrola osoby, której dane dotyczą, staje się iluzoryczna, a zgoda stanowi nieodpowiednią podstawę przetwarzania.

Wśród swoich zaleceń Grupa Robocza nalega na potrzebę wyjaśnienia, co oznacza ‘jednoznaczna zgoda’: "Celem wyjaśnienia powinno być podkreślenie, że jednoznaczna zgoda wymaga użycia mechanizmów niepozostawiających wątpliwości co do zamiaru wyrażenia zgody przez osobę, której dane dotyczą. Jednocześnie należy jasno wskazać, że wykorzystanie domyślnych ustawień, które osoba, której dane dotyczą, musi zmodyfikować, aby odmówić przetwarzania (zgoda oparta na milczeniu), nie stanowi samo w sobie jednoznacznej zgody. Jest tak zwłaszcza w środowisku internetowym." [34] Wymaga również od administratorów danych wprowadzenia mechanizmów umożliwiających wykazanie zgody (w ramach ogólnego obowiązku rozliczalności) oraz wymaga od ustawodawcy dodania wyraźnego wymogu dotyczącego jakości i dostępności informacji stanowiących podstawę zgody.

[33] Oczywiste jest, że również w przypadku zastosowania artykułu 8 należy zapewnić przestrzeganie innych przepisów dyrektywy, w tym artykułu 6.
[34] Patrz strona 36 opinii Grupy Roboczej 15/2011 w sprawie definicji zgody.

III.2.2. Umowa

Artykuł 7 lit. b) stanowi podstawę prawną w sytuacjach, gdy ‘przetwarzanie jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy. Obejmuje to dwa różne scenariusze.

i) Po pierwsze, przepis dotyczy sytuacji, gdy przetwarzanie jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą. Może to np. dotyczyć przetwarzania adresu osoby, której dane dotyczą, tak aby możliwa była dostawa towarów zakupionych online, lub przetwarzania informacji dotyczących karty kredytowej w celu realizacji płatności. W kontekście zatrudnienia podstawa ta może na przykład pozwolić na przetwarzanie informacji na temat wynagrodzenia oraz informacji dotyczących konta bankowego, tak aby można było wypłacić wynagrodzenie.

   Przepis należy interpretować ściśle i nie może on odnosić się do sytuacji, w których przetwarzanie nie jest rzeczywiście *konieczne* dla realizacji umowy, ale raczej jest jednostronnie nałożone na osobę, której dane dotyczą, przez administratora. Także fakt, że niektóre operacje przetwarzania danych są objęte umową, nie oznacza automatycznie, że przetwarzanie jest konieczne dla jej realizacji. Na przykład artykuł 7 lit. b) nie jest odpowiednią podstawą prawną do stworzenia profilu użytkownika dotyczącego jego wyborów dokonywanych w związku z upodobaniami i stylem życia w oparciu o odwiedzane strony internetowe i kupowane produkty. Jest tak, ponieważ administratorowi danych nie zlecono do prowadzenia profilowania, ale raczej np. dostarczenie określonych dóbr i usług. Nawet jeżeli te operacje przetwarzania są konkretnie wskazane małym drukiem w umowie, sam ten fakt nie czyni ich ‘koniecznymi’ dla realizacji umowy.

   Istnieje wyraźne powiązanie między oceną konieczności i zgodności z zasadą ograniczenia celu. Ważne jest ustalenie dokładnych *racjonalnych podstaw* umowy, tj. jej istoty i podstawowego celu, ponieważ w odniesieniu do tego będzie przeprowadzany test, czy przetwarzanie danych jest konieczne dla jej realizacji.

   W niektórych sytuacjach granicznych ustalenie, czy przetwarzanie jest konieczne dla realizacji umowy, może być sporne lub może wymagać ustalenia bardziej konkretnych faktów. Na przykład utworzenie ogólnofirmowej wewnętrznej bazy danych kontaktowych pracowników zawierającej nazwisko, adres firmowy, numer telefonu oraz adres e-mail wszystkich pracowników, w celu umożliwienia pracownikom kontaktu ze swoimi kolegami, może w niektórych sytuacjach być uznawane za konieczne dla realizacji umowy na mocy artykułu 7 lit. b), ale może być również legalne na mocy artykułu 7 lit. f), jeżeli wykazany zostanie nadrzędny interes administratora i podjęte zostaną wszystkie odpowiednie środki, w tym na przykład przeprowadzenie odpowiednich konsultacji z przedstawicielami pracowników.

   Inne przypadki, na przykład elektroniczny monitoring wykorzystywania przez pracownika Internetu, poczty e-mail czy też telefonu, bądź wideonadzór pracowników bardziej ewidentnie stanowią przetwarzanie, co do którego istnieje prawdopodobieństwo, że wykracza ponad to, co jest konieczne dla realizacji umowy o pracę, mimo że w tym przypadku również może to zależeć od charakteru pracy.

Zapobieganie oszustwom – które może obejmować między innymi monitorowanie i profilowanie klientów – jest innym typowym obszarem, który może prawdopodobnie być uznany za wykraczający ponad to, co jest konieczne dla realizacji umowy. Takie przetwarzanie nadal może być legalne w oparciu o inną podstawę z artykułu 7, na przykład zgodę, gdy to właściwe, zobowiązanie prawne lub prawnie uzasadniony interes administratora (artykuł 7 lit. a), c) lub f)).[35] W tym ostatnim przypadku przetwarzanie powinno podlegać dodatkowym gwarancjom i środkom, aby odpowiednio chronić interesy lub prawa i wolności osób, których dane dotyczą.

Artykuł 7 lit. b) ma zastosowanie tylko do tego, co jest konieczne dla realizacji umowy. Nie ma zastosowania do wszystkich dalszych działań wywołanych przez niezapewnienie zgodności lub do wszelkich innych incydentów przy realizacji umowy. Dopóki przetwarzanie obejmuje normalną realizację umowy, może podlegać artykułowi 7 lit. b). Jeżeli ma miejsce incydent w realizacji, który wywołuje konflikt, przetwarzanie danych może obrać inny kierunek. Przetwarzanie podstawowych informacji na temat osoby, której dane dotyczą, takich jak nazwisko, adres i odniesienie do zaległych zobowiązań umownych, w celu wysyłania przypomnień nadal powinno być uznawane za przetwarzanie danych konieczne dla realizacji umowy. W odniesieniu do bardziej złożonego przetwarzania danych, które może obejmować strony trzecie lub nie, np. do zewnętrznej windykacji długów czy wezwania do sądu klienta, który nie zapłacił za usługę, można by argumentować, że takie przetwarzanie nie ma już miejsca w ramach 'normalnej' realizacji umowy i w związku z tym nie podlega artykułowi 7 lit. b). Jednakże nie spowoduje to, że przetwarzanie będzie nielegalne jako takie: administrator ma prawnie uzasadniony interes, aby szukać środków prawnych w celu zapewnienia, że szanowane będą jego prawa umowne. Można polegać na innych podstawach prawnych, takich jak artykuł 7 lit. f), z zastrzeżeniem odpowiednich gwarancji i środków i przy spełnieniu testu równowagi.[36]

ii) Po drugie, artykuł 7 lit. b) dotyczy również przetwarzania, które ma miejsce *przed* zawarciem umowy. Chodzi o relacje przed zawarciem umowy, pod warunkiem podjęcia kroków raczej na wniosek osoby, której dane dotyczą, a nie z inicjatywy administratora czy strony trzeciej. Na przykład, jeżeli osoba zwraca się do sprzedawcy detalicznego o przesłanie jej oferty produktu, przetwarzanie w tych celach, np. przechowywanie informacji dotyczących adresu i tego, o co się zwrócono, przez ograniczony czas, będzie właściwie w oparciu o tę podstawę prawną. Podobnie, jeżeli osoba zwraca się do ubezpieczyciela o wycenę swojego samochodu, ubezpieczyciel może przetwarzać potrzebne dane, na przykład marka i rok produkcji samochodu, jak również inne istotne i proporcjonalne dane, w celu przygotowania wyceny.

---

[35] Inny przykład licznych podstaw prawnych można znaleźć w opinii Grupy Roboczej 15/2011 w sprawie definicji zgody (wskazanej w przypisie 2). W celu zakupu samochodu administrator danych może być uprawniony do przetwarzania danych osobowych zgodnie z różnymi celami i w oparciu o różne podstawy:
- dane konieczne do zakupu samochodu: artykuł 7 lit. b),
- przetwarzanie dokumentów samochodu: artykuł 7 lit. c),
- do celów usług zarządzania relacjami z klientami (np. aby możliwy był serwis samochodu w różnych filiach firmy w UE); artykuł 7 lit. f),
- W celu przekazania danych stronom trzecim do celów ich własnych działań marketingowych: artykuł 7 lit. a).

[36] W odniesieniu do szczególnych kategorii danych, może istnieć potrzeba wzięcia pod uwagę również artykułu 8 ust. 1 lit. e) - 'konieczne do ustalenia, wykonania lub ochrony roszczeń prawnych.

Jednakże szczegółowe weryfikacje, na przykład przetwarzanie danych dotyczących badań lekarskich zanim przedsiębiorstwo ubezpieczeniowe zapewni wnioskodawcy ubezpieczenie zdrowotne lub ubezpieczenie na życie nie będą uważane za konieczne kroki podejmowane na wniosek osoby, której dane dotyczą. Weryfikacja wiarygodności kredytowej przed udzieleniem pożyczki również nie jest przeprowadzana na *wniosek* osoby, której dane dotyczą, na mocy artykułu 7 lit. b), ale raczej, na mocy artykułu 7 lit. f) lub artykułu 7 lit. c) zgodnie z zobowiązaniem prawnym banków do sprawdzenia oficjalnej listy zarejestrowanych dłużników.

Marketing bezpośredni z inicjatywy sprzedawcy detalicznego/administratora również nie będzie możliwy na tej podstawie. W niektórych przypadkach artykuł 7 lit. f) może stanowić odpowiednią podstawę prawną zamiast artykułu 7 lit. b), z zastrzeżeniem odpowiednich gwarancji i środków, oraz przy spełnieniu testu równowagi. W innych przypadkach, w tym tych dotyczących obszernego profilowania, wymiany danych, marketingu bezpośredniego online czy też reklamy behawioralnej, powinna być rozważona zgoda na mocy artykułu 7 lit. a), jak wynika z analizy przedstawionej poniżej.[37]

III.2.3. Zobowiązanie prawne

Artykuł 7 lit. c) stanowi podstawę prawną w sytuacjach, gdy ‘przetwarzanie jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega’. Może to mieć na przykład miejsce, gdy pracodawca musi przekazywać dane na temat wynagrodzeń swoich pracowników do organów ubezpieczenia społecznego lub organów podatkowych bądź gdy instytucje finansowe są zobowiązane do zgłaszania określonych podejrzanych transakcji właściwym organom na mocy przepisów odnoszących się do zapobiegania praniu brudnych pieniędzy. Może być to również zobowiązanie, któremu podlega organ publiczny, ponieważ nic nie ogranicza zastosowania artykułu 7 lit. c) do sektora prywatnego lub publicznego. Będzie to miało zastosowanie np. do gromadzenia danych przez organ lokalny w celu zajęcia się grzywnami za parkowanie w niedozwolonych miejscach.

Artykuł 7 lit. c) wykazuje podobieństwa z artykułem 7 lit. e), ponieważ zadanie w interesie publicznym często oparte jest na lub wywodzi się z przepisu prawnego. Zakres artykułu 7 lit. c) jest jednakże ściśle ograniczony.

Aby artykuł 7 lit.(c) miał zastosowanie, zobowiązanie musi być nałożone przez prawo (a nie na przykład przez umowę). Prawo musi spełniać wszystkie istotne warunki, aby uczynić zobowiązanie ważnym i wiążącym, jak również musi być zgodny z prawem ochrony danych, w tym z wymogiem konieczności, proporcjonalności[38] i ograniczenia celu.

Ważne jest również, aby podkreślić, że artykuł 7 lit. c) odnosi się do przepisów Unii Europejskiej lub państwa członkowskiego. Zobowiązania wynikające z przepisów krajów trzecich (takie jak np. obowiązek tworzenia programów zgłaszania nieprawidłowości na mocy ustawy Sarbanes–Oxley z 2002 r. w Stanach Zjednoczonych) nie są objęte tą podstawą. Aby było ważne, zobowiązanie prawne kraju trzeciego musiałoby być oficjalnie uznane i włączone do porządku prawnego danego państwa członkowskiego, na przykład w formie

[37] Patrz część III.3.6 (b) ' Przykład: ewolucja podejścia do marketingu bezpośredniego ' na str. 45-46.

[38] Patrz także opinia Grupy Roboczej 1/2014 w sprawie zastosowania koncepcji niezbędności i proporcjonalności oraz ochrony danych w sektorze egzekwowania prawa, przyjęta 27.02.2014 r. (WP 211).

międzynarodowej umowy[39]. Z drugiej strony konieczność wykonania zagranicznego zobowiązania prawnego może stanowić prawnie uzasadniony interes administratora, ale jedynie z zastrzeżeniem testu równowagi z artykułu 7 lit. f) i pod warunkiem wprowadzenia odpowiednich gwarancji, takich jak te zatwierdzone przez właściwy organ ochrony danych.

Administrator nie może mieć wyboru, czy wykonać zobowiązanie czy też nie. Zatem artykuł 7 lit. c) nie ma zastosowania do dobrowolnych jednostronnych przedsięwzięć i partnerstw publiczno-prawnych i przetwarzania w ich ramach danych wykraczając ponad to, co jest wymagane prawem. Na przykład jeżeli – bez wyraźnego, konkretnego zobowiązania prawnego do uczynienia tego – dostawca usług internetowych postanawia monitorować swoich użytkowników, dążąc do zwalczania nielegalnego pobierania, artykuł 7 lit. c) nie będzie odpowiednią podstawą prawną do tego celu.

Ponadto samo zobowiązanie prawne musi wystarczająco jasno określać wymagane przetwarzanie danych. Zatem artykuł 7 lit. c) ma zastosowanie na podstawie przepisów prawnych wyraźnie odnoszących się do charakteru i przedmiotu przetwarzania. Administrator nie powinien posiadać nienależytego stopnia swobody co do tego, jak należy wykonać zobowiązanie prawne.

W niektórych przypadkach ustawodawstwo może określać tylko ogólny cel, podczas gdy bardziej szczegółowe zobowiązania są nakładane na innym poziomie, na przykład albo w aktach wykonawczych albo na mocy wiążącej decyzji organu publicznego w konkretnym przypadku. Może to również prowadzić do zobowiązań prawnych na mocy artykułu 7 lit. c), pod warunkiem że charakter i przedmiot przetwarzania jest dobrze określony i z zastrzeżeniem odpowiedniej podstawy prawnej.

Jednak inaczej jest, gdy organ regulacyjny zapewnia tylko ogólne wytyczne co do polityki i warunki, pod którymi mógłby rozważyć użycie swoich uprawnień egzekucyjnych (np. wytyczne regulacyjne dla instytucji finansowych dotyczące określonych standardów należytej staranności). W takich przypadkach operacje przetwarzania powinny być ocenione na mocy artykułu 7 lit. f) oraz być uznane za legalne jedynie z zastrzeżeniem dodatkowego testu równowagi.[40]

W ramach ogólnej uwagi, należy zaznaczyć, że może się wydawać, iż niektóre operacje przetwarzania są bliskie podleganiu pod artykuł 7 lit. c) lub artykuł 7 lit. b), bez spełnienia całkowicie kryteriów zastosowania dla tych podstaw. Nie oznacza to, że takie przetwarzanie jest zawsze koniecznie zgodne z prawem: czasami może być legalne, ale raczej na mocy artykułu 7 lit. f), z zastrzeżeniem dodatkowego testu równowagi.

[39] Patrz w tej kwestii część 4.2.2 opinii Grupy Roboczej 10/2006 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Worldwide Interbank Financial Telecommunication, SWIFT), przyjętej 20.11.2006 r. (WP128) oraz opinia Grupy Roboczej 1/2006 w sprawie zastosowania unijnych zasad ochrony danych do wewnętrznych systemów informowania o nieprawidłowościach w dziedzinie księgowości, wewnętrznych kontroli księgowych, spraw związanych z audytem, zwalczania przekupstwa oraz przestępstw bankowych i finansowych, przyjęta 01.02.2006 r. (WP 117).

[40] Wytyczne organu regulacyjnego nadal mogą odgrywać role w ocenie prawnie uzasadnionego interesu administratora (patrz część III.3.4 punkt (a), szczególnie strona 36).

III.2.4. Żywotny interes

Artykuł 7 lit. (d) przewiduje podstawę prawna w sytuacjach, gdy ‘przetwarzanie jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą’. To sformułowanie różni się od języka użytego w artykule 8 ust. 2 lit. c, który jest bardziej konkretny i odnosi się do sytuacji, gdy ‘przetwarzanie jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby, w przypadku gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do udzielenia zgody’.

Niemniej wydaje się, że oba przepisy sugerują, iż ta podstawa prawna powinna mieć ograniczone zastosowanie. Po pierwsze wydaje się, że zwrot ‘żywotny interes’ ogranicza stosowanie tej podstawy do kwestii życia i śmierci lub, co najmniej, zagrożeń, które stanowią ryzyko obrażenia lub uszczerbku dla zdrowia osoby, której dane dotyczą (lub w przypadku artykułu 8 ust. 2 lit. c) również innej osoby).

Motyw 31 potwierdza, że celem tej podstawy prawnej jest ‘ochrona interesu, który jest niezbędny dla życia osoby, której dane dotyczą’. Jednak dyrektywa nie określa dokładnie, czy zagrożenie musi być bezpośrednie. Podnosi to kwestie dotyczące zakresu gromadzenia danych, na przykład jako środek prewencyjny lub na szeroką skalę, jak np. gromadzenie danych pasażerów linii lotniczych, gdy zidentyfikowano ryzyko choroby epidemiologicznej lub incydentu w zakresie ochrony lotnictwa cywilnego.

Grupa Robocza uważa, że przepis ten wymaga restrykcyjnej interpretacji, zgodnej z duchem artykułu 8. Mimo że artykuł 7 lit. d) nie ogranicza konkretnie wykorzystywania tej podstawy w sytuacjach, gdy nie można wykorzystać zgody jako podstawy prawnej, ze względów określonych w artykule 8 ust. 2 lit. c), rozsądne będzie założenie, że w sytuacjach, w których istnieje możliwość i potrzeba żądania ważnej zgody, w istocie należy dążyć do uzyskania zgody zawsze, gdy jest to wykonalne. Ograniczy to również stosowanie tego przepisu w przypadku analizy dla konkretnego przypadku i nie może być normalnie wykorzystywane w celu legitymizacji masowego gromadzenia lub przetwarzania danych osobowych. W przypadku, gdy byłoby to konieczne, artykuł 7 lit. c) lub e) byłyby bardziej odpowiednimi podstawami przetwarzania.

III.2.5. Zadanie publiczne

Artykuł 7 lit. e) stanowi podstawę prawną w sytuacjach, gdy ‘przetwarzanie jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane‘.

Koniecznie należy zauważyć, że podobnie jak artykuł 7 lit. c), artykuł 7 lit. e) odnosi się do interesu publicznego Unii Europejskiej lub państwa członkowskiego. Podobnie ‘publiczna władza’ odnosi się do władzy przyznanej przez Unię Europejską lub państwo członkowskie. Innymi słowy, zadania realizowane w interesie publicznym kraju trzeciego lub dla wykonywania władzy publicznej przyznanej na mocy prawa zagranicznego, które nie podlega zakresowi tego przepisu.[41]

Artykuł 7 lit. e) dotyczy dwóch sytuacji i jest właściwy zarówno dla sektora publicznego, jak i prywatnego. Po pierwsze, dotyczy sytuacji, gdy sam administrator danych ma władzę publiczną lub zadanie w interesie publicznym (ale niekoniecznie także prawny obowiązek przetwarzania danych), a przetwarzanie jest konieczne dla realizacji tej władzy lub wykonania tego zadania. Na przykład organ podatkowy może gromadzić i przetwarzać zeznanie podatkowe osoby w celu ustalenia i weryfikacji kwoty podatku, jaką należy zapłacić, albo profesjonalne stowarzyszenie, takie jak stowarzyszenie adwokackie lub izba lekarska, któremu przyznano władzę publiczną umożliwiającą prowadzenie postępowań dyscyplinarnych wobec niektórych z ich członków. Jeszcze innym przykładem mógłby być organ samorządowy, taki jak władze miejskie, którym powierzono zadanie prowadzenia usług bibliotecznych, szkoły czy lokalnego basenu.

Po drugie, artykuł 7 lit. e) dotyczy również sytuacji, gdy administrator nie ma publicznej władzy, ale jest proszony przez stronę trzecią posiadającą taką władzę o udostępnienie danych. Na przykład urzędnik organu publicznego odpowiedzialny za prowadzenie dochodzeń w sprawie przestępstw może raczej poprosić administratora o współpracę przy trwającym dochodzeniu, a nie żądać od administratora spełnienia określonej prośby o współpracę. Artykuł 7 lit. e) może ponadto dotyczyć sytuacji, w których administrator proaktywnie udostępnia dane stronie trzeciej posiadającej taką władzę publiczną. Może mieć to na przykład miejsce, gdy administrator zauważy, że popełniono przestępstwo i przekaże te informacje właściwym organom w zakresie egzekwowania prawa z własnej inicjatywy.

W przeciwieństwie do przypadku z artykułu 7 lit. c), nie ma wymogu, aby administrator działał na podstawie zobowiązania prawnego. Nawiązując do poprzedniego przykładu, administrator, który przypadkowo zauważy, że popełniono kradzież lub oszustwo, nie może na podstawie zobowiązania prawnego zgłosić tego policji, ale niemniej może, w odpowiednich przypadkach, uczynić to dobrowolnie na podstawie artykułu 7 lit. e).

Jednakże przetwarzanie musi być ‘konieczne dla realizacji zadania wykonywanego w interesie publicznym’. Ewentualnie albo administrator danych albo strona trzecia, której

[41] W kwestii podobnej interpretacji pojęcia ‘ważnych względów publicznych’ w artykule 26 ust. 1 lit. d) patrz część 2.4 dokumentu roboczego Grupy Roboczej dotyczącego wspólnej wykładni artykułu 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r., przyjętego 25 listopada 2005 r. (WP 114).

administrator udostępnia dane, musi posiadać władzę publiczną, a przetwarzanie danych musi być konieczne dla realizacji tej władzy'.[42] Należy również koniecznie podkreślić, że ta publiczna władza lub zadanie publiczne zazwyczaj są przypisywane w ustawach lub innych przepisach prawnych. Jeżeli przetwarzanie oznacza naruszenie prywatności lub na mocy prawa krajowego wymagane jest zapewnienie ochrony osób, których dane dotyczą, podstawa prawna powinna być wystarczająco konkretna i dokładna, jeżeli chodzi o określenie przetwarzania danych, które może być dozwolone.

Sytuacje te stają się coraz bardziej powszechne, także poza ramami sektora publicznego, uwzględniając tendencję do powierzania zadań rządowych podmiotom w sektorze prywatnym. Może mieć to np. miejsce w kontekście operacji przetwarzania w sektorze transportowym lub sektorze opieki zdrowotnej (np. badania epidemiologiczne, badania). Podstawę tę można również przytoczyć w kontekście egzekwowania prawa, co już sugerowano w przykładzie wskazanym powyżej. Jednak zakres, w jakim prywatnemu przedsiębiorstwu można pozwolić na współpracę z organami egzekwowania prawa, na przykład w walce z oszustwami i nielegalnymi treściami w Internecie, wymaga analizy nie tylko w związku artykułem 7, ale także artykułem 6, uwzględniając wymogi ograniczenia celu, zgodności z prawem oraz rzetelności[43].

Artykuł 7 lit. e) ma potencjalnie bardzo szeroki zakres stosowania, który przemawia za ścisłą interpretacją i wyraźnym określeniem, dla konkretnych przypadków, przedmiotowego interesu publicznego oraz władzy publicznej uzasadniającej przetwarzanie. Ten szeroki zakres wyjaśnia również, dlaczego, tak jak w przypadku artykułu 7 lit. f), przewidziano prawo do wyrażenia sprzeciwu w artykule 14, gdy przetwarzanie oparte jest na artykule 7 lit. e)[44]. Podobne gwarancje i środki dodatkowe muszą mieć zastosowanie w obu przypadkach [45].

W tym rozumieniu artykuł 7 lit. e) wykazuje podobieństwa z artykułem 7 lit. f), w niektórych kontekstach, szczególnie dla organów publicznych, artykuł 7 lit. e) może zastąpić artykuł 7 lit. f).

Oceniając zakres tych przepisów dla organów sektora publicznego, szczególnie w świetle proponowanych zmian w ramach prawnych ochrony danych, warto zauważyć, że obecny tekst rozporządzenia 45/2001,[46] które zawiera zasady ochrony danych mające zastosowanie wobec instytucji i organów Unii Europejskiej, nie ma przepisu porównywalnego do artykułu 7 lit. f).

Jednakże, motyw 27 niniejszego Rozporządzenia stanowi, że „przetwarzanie danych osobowych w celu przeprowadzenia czynności wykonywanych *w interesie ogólnym* przez

[42] Innymi słowy, w tych przypadkach nadal będą miały miejsce publiczne znaczenie tych zadań oraz związana z tym odpowiedzialność, nawet jeżeli wykonanie zadania przeniesiono na inne podmioty, w tym prywatne.

[43] W tym rozumieniu patrz opinia Grupy Roboczej w sprawie SWIFT (wskazana w przypisie 39 powyżej), opinia Grupy Roboczej 4/2003 w sprawie poziomu ochrony zapewnionego w USA dla przekazywania danych pasażerów, przyjęta 13.06.2003 r. (WP78) oraz dokument roboczy w sprawie kwestii ochrony danych dotyczących praw własności intelektualnej, przyjęty 18.01.2005 r. (WP 104).

[44] Jak wskazano powyżej, ta możliwość wyrażenia sprzeciwu nie istnieje w niektórych państwach członkowskich (np. Szwecji) w przypadku przetwarzania danych w oparciu o artykuł 7 lit. e).

[45] Jak pokazano poniżej, projekt sprawozdania Komisji LIBE sugeruje dalsze gwarancje, w szczególności większą przejrzystość, dla przypadku, gdy ma zastosowanie artykuł 7 lit. f).

[46] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe oraz o swobodnym przepływie takich danych (Dz. Urz. L 8, 12.1.2001, str. 1).

instytucje i organy wspólnotowe obejmuje przetwarzanie danych osobowych niezbędnych dla zarządzania i funkcjonowania tych instytucji i organów." W ten sposób, powyższy przepis pozwala na przetwarzanie danych na podstawie szeroko interpretowanego pojęcia „czynności w interesie ogólnym", obejmującego wielką liczbę przypadków, które w innym razie podlegałyby przepisom podobnym do artykułu 7 lit. f). Monitoring wizyjny pomieszczeń dla celów bezpieczeństwa, monitoring elektroniczny przepływu poczty elektronicznej lub ocena pracowników stanowią jedynie kilka przykładów tego, co może podlegać szeroko interpretowanemu przepisowi na temat „czynności wykonywanych *w interesie ogólnym".*

Spoglądając w przyszłość, równie ważne jest rozważenie tego, że proponowane Rozporządzenie, w artykule 6 ust. 1 lit. f) szczegółowo stanowi, że przesłanki prawnie uzasadnionego interesu „nie stosuje się do przetwarzania realizowanego przez organy publiczne w wykonaniu ich zadań". Jeżeli przepis ten zostanie przyjęty i będzie szeroko interpretowany, tak aby wykluczyć możliwość stosowania przez instytucje publiczne prawnie uzasadnionego interesu jako podstawy prawnej, wtedy podstawy o których mowa w art. 6 lit. e), tj. „interes ogólny" oraz „organy publiczne", będą musiały być interpretowane w taki sposób, aby zezwolić organom publicznym na pewną dozę elastyczności, przynajmniej aby zapewnić właściwe nimi zarządzenie oraz ich właściwe funkcjonowanie, tak jak obecnie jest interpretowane Rozporządzenie 45/2001.

Opcjonalnie, przywołane tutaj ostatnie zdanie artykułu 6 ust. 1 lit. f) Rozporządzenia, mogłoby być interpretowane taki sposób, aby nie wykluczać możliwości zastosowania prawnie uzasadnionego interesu jako podstawy prawnej przez organy publiczne. W takim przypadku, sformułowanie „przetwarzanie danych osobowych w celu przeprowadzenia czynności wykonywanych *w interesie ogólnym"* w proponowanym art. 6 ust. 1 lit. f), powinno być interpretowane wąsko. Taka wąska interpretacja oznaczałaby, że przetwarzanie dla celów właściwego zarządzania oraz funkcjonowania tych organów publicznych nie mieściłoby się w zakresie „przetwarzania realizowanego przez organy publiczne w wykonaniu ich zadań". W rezultacie, przetwarzanie dla celów właściwego zarządzania oraz funkcjonowania tych organów publicznych mogłoby wciąż być możliwe na podstawie prawnie uzasadnionego interesu.

III.3. Artykuł 7 lit. f): prawnie uzasadnione interesy

Artykuł 7 lit. f)[47] wzywa do testu równowagi: prawnie uzasadnione interesy administratora (lub stron trzecich) musi być wyważony względem interesów związanych z podstawowymi prawami i wolnościami osoby, której dane dotyczą. Rezultat testu równowagi w dużym stopniu określa, czy można oprzeć się na art. 7 lit. f) jako na podstawie przetwarzania.

Już na tym etapie warto wspomnieć, że nie jest to prosty test równowagi, który składałby się po prostu z dwóch łatwo policzalnych oraz łatwo porównywalnych „miar". Raczej, jak zostanie to opisane bardziej szczegółowo poniżej, przeprowadzenie testu równowagi może wymagać kompleksowej oceny, biorącej pod uwagę dużą liczbę czynników. W celu pomocy w ustrukturalizowaniu oraz ułatwieniu oceny, podzieliliśmy proces na kilka kroków, tak aby pomóc zapewnić, że test równowagi może być skutecznie przeprowadzony.

[47] Aby zobaczyć cały tekst art. 7 lit. f) patrz str. 4 powyżej.

Część III.3.1. na początku analizuje jedną ze stron testu równowagi: co stanowi (prawnie) „uzasadniony interes administratora danych lub osoby trzeciej, którym dane osobowe są udostępniane". W części III.3.2., przeanalizujemy drugą stronę testu równowagi, co stanowi „interes związany z podstawowymi prawami i wolnościami osoby, której dane dotyczą, których ochrona jest gwarantowana na podstawie art. 1 ust. 1".

W częściach III.3.3 oraz III.3.4 zawarto wytyczne na temat tego, jak przeprowadzać test równowagi. Część III.3.3. zawiera ogólny wstęp, posiłkujący się trzema odmiennymi scenariuszami. W następstwie tego wstępu, Część III.3.4 nakreśla najistotniejsze uwagi, które muszą być wzięte pod uwagę przy przeprowadzaniu testu równowagi, włączając w to zabezpieczenia oraz środki zapewnione przez administratora danych.

W częściach III.3.5 oraz III.3.6 przyjrzymy się na koniec niektórym poszczególnym mechanizmom, takim jak rozliczalność, przejrzystość oraz prawo do sprzeciwu, które mogą pomóc zapewnić- oraz dalej wzmocnić – właściwą równowagę pomiędzy różnymi interesami, które mogą znaleźć się na szali.

III.3.1. Prawnie uzasadnione interesy administratora (lub stron trzecich)

Pojęcie „interesu"

Pojęcie „interesu" jest ściśle powiązane, jednakże różne od pojęcia „celu" wspomnianego w art. 6 dyrektywy. W dyskursie na temat ochrony danych, „cel" jest konkretnym powodem, dla którego dane są przetwarzane: cel lub intencja przetwarzania danych. Interes, z drugiej strony, jest szerszym powodem, który administrator danych może posiadać, aby przetwarzać dane, lub korzyścią, którą administrator osiąga – lub społeczeństwo może osiągnąć – na skutek przetwarzania.

Na przykład, firma może mieć interes w zapewnieniu zastosowania zasad bhp swoich pracowników w elektrowni atomowej. W związku z tym, *celem* firmy może być wdrożenie konkretnej procedury kontroli dostępu, która uzasadnia przetwarzania pewnych określonych danych osobowych w celu pomocy w zapewnieniu zastosowania zasad bhp przez pracowników.

Interes musi być wystarczająco jasno wyrażony, tak aby pozwolić na przeprowadzenie testu równowagi względem interesów oraz praw podstawowych osoby, której dane dotyczą. Ponadto musi to być „interes administratora". Wymaga to aby interes był rzeczywisty i obecny, czymś co odpowiada aktualnym działalnościom lub korzyściom, które są oczekiwane w bardzo bliskiej przyszłości. Innymi słowy, interes, który będzie zbyt ogólny lub spekulatywny, nie będzie wystarczający.

Charakter interesu może być różny. Niektóre interesy mogą być istotne lub z korzyścią dla całego społeczeństwa, tak jak interes prasy do publikowania informacji na temat korupcji w rządzie lub interes w prowadzeniu badań naukowych (przy zastosowaniu odpowiednich środków ochronnych). Inne interesy mogą mieć mniejszy wpływ na społeczeństwo jako całość, lub w każdym razie, ich wpływ na społeczeństwo może być bardziej mieszany lub kontrowersyjny. Może to np. dotyczyć ekonomicznego interesu firmy, aby dowiedzieć się jak najwięcej na temat jej potencjalnych klientów, tak aby mogła lepiej ukierunkować reklamę swoich produktów lub usług.

Co czyni interes prawnie uzasadnionym lub nieuzasadnionym?

Celem tego pytania jest określenie progu, którego przekroczenie czyni interes prawnie uzasadnionym. Jeżeli interes administratora danych jest nieuzasadniony, test równowagi nie będzie wchodzić w grę, jako że wstępny próg dla zastosowania art. 7 lit. f) nie został osiągnięty.

W opinii Grupy Roboczej pojęcie prawnie uzasadnionego interesu może obejmować szeroki zakres interesów, czy to błahych czy bardzo istotnych, jasnych lub bardziej kontrowersyjnych. Tak więc to w drugim kroku dojdzie do porównania tych interesów z interesami oraz prawami podstawowymi osób, których dane dotyczą, gdzie będzie musiałoby być zastosowane bardziej restrykcyjne podejście oraz pełniejsza analiza.

Poniżej wskazano niewyczerpującą listę niektórych najczęstszych kontekstów, w których może pojawić się kwestia prawnie uzasadnionego interesu w znaczeniu art. 7 lit. f). Jest ona przedstawiona, bez uszczerbku dla kwestii tego, czy interes administratora ostatecznie będzie nadrzędny wobec interesów oraz praw osób, których dane dotyczą, przy przeprowadzaniu testu równowagi.

- wykorzystanie prawa do wolności wypowiedzi lub informacji, w tym w mediach i sztuce
- konwencjonalny marketing bezpośredni oraz inne formy marketingu lub reklamy
- niezamówione informacje niehandlowe, włączając w to kampanie wyborcze lub zbieranie środków na cele charytatywne
- egzekucja roszczeń prawnych, włączając w to zbieranie długów poprzez procedury pozasądowe
- zapobieganie oszustwom, niewłaściwemu korzystaniu z usług, lub praniu pieniędzy
- monitoring pracowników dla celów bezpieczeństwa lub zarządzania
- systemu informowania o nieprawidłowościach
- bezpieczeństwo fizyczne, informatyczne oraz sieciowe
- przetwarzanie dla celów badań historycznych, naukowych lub statystycznych
- przetwarzanie dla celów badań (włączając badania rynkowe)

Odpowiednio, interes może być uznany za prawnie uzasadniony tak długo jak długo administrator może do niego dążyć w sposób zgodny z prawem ochrony danych oraz innymi przepisami. Innymi słowy, prawnie uzasadniony interes musi być „do zaakceptowania w świetle prawa".[48]

[48] Uwagi na temat charakteru „zgodności z prawem" z Części III.1.3. Opinii Grupy Roboczej 3/2013 w sprawie ograniczenia celu, znajdują także zastosowanie tutaj mutatis mutandis. Tak jak na stronie 19 Opinii „pojęcie „prawa" jest tutaj użyte w szerszym kontekście. Obejmuje to inne prawa właściwe, takie jak prawa dotyczące zatrudnienia, umów lub prawo ochrony konsumentów. Co więcej, pojęcie prawa obejmuje wszystkie formy pisemnego oraz zwyczajowego prawa, prawo pierwotne oraz akty wykonawcze, akty lokalne, precedensy prawne, zasady konstytucyjne, inne zasady prawne jak również właściwość sądów, ponieważ takie „prawo"

Z tego względu, aby być ‘prawnie uzasadnionym’ w świetle art. 7 lit. f), interes musi:

- być zgodny z prawem (tj. zgodny z właściwym prawem UE oraz prawem krajowym);
-być wystarczająco jasno wyrażony, tak aby pozwolić na zastosowanie testu równowagi względem interesów oraz praw podstawowych osoby, której dane dotyczą (tj. wystarczająco konkretny)
- musi być rzeczywisty i obecny (nie spekulatywny)

Okoliczność, że administrator posiada taki prawnie uzasadniony interes w przetwarzaniu pewnych danych, nie oznacza, że musi on koniecznie opierać się na art. 7 lit. f), jako podstawie prawnej przetwarzania. Zasadność interesu administratora danych jest jedynie punktem wyjścia, jednym z elementów, który musi być przeanalizowany zgodnie z art. 7 lit. f), To czy można oprzeć się na art. 7 lit. f) będzie zależeć od wyniku testu równowagi, który następuje.

W celu zobrazowania: administratorzy mogą mieć prawnie uzasadniony interes w poznaniu preferencji swoich klientów, tak aby umożliwić im lepsze spersonalizowanie ofert, a docelowo, zaoferować produkty oraz usługi, które lepiej spełniają potrzeby oraz pragnienia klientów. W tym świetle, art. 7 lit. f) może być odpowiednią podstawą prawną do wykorzystania do niektórych rodzajów działań marketingowych, zarówno on-line jak i off-line, przy zapewnieniu odpowiednich środków ochronnych (włączając w to, m.in., działający mechanizm polegający na zgłoszeniu sprzeciwu wobec takiego przetwarzania, zgodnie z art. 14 lit. b), jak zostanie to pokazane w Części III.3.6 *Prawo do sprzeciwu oraz prawa wykraczające poza nie).*

Jednakże nie oznacza to, że administratorzy mogliby oprzeć się na art. 7 lit. f), aby przesadnie monitorować czynności on-line lub off-line swoich klientów, zestawiać wielkie ilości danych na ich temat z różnych źródeł, które pierwotnie były zebrane w innych kontekstach oraz dla innych celów, oraz utworzyć –i, na przykład, za pośrednictwem osób handlujących danymi, także sprzedawać – całościowe profile osobowości swoich klientów oraz preferencji bez ich wiedzy, wykonalnego mechanizmu sprzeciwu, nie mówiąc już o świadomej zgodzie. Jest prawdopodobne, że takie profilowanie stanowi poważne naruszenie prywatności klienta, i kiedy się to dzieje, interesy oraz prawa osoby, której dane dotyczą, byłyby nadrzędne wobec interesu administratora.[49]

Jako kolejny przykład, w swojej opinii na temat SWIFT[50], chociaż Grupa Robocza uznała prawnie uzasadniony interes firmy w podporządkowaniu się pozwom, zgodnie z prawem USA, tak aby uniknąć sankcji ze strony instytucji USA, uznała także, że nie można oprzeć się

---

byłoby interpretowane oraz brane pod uwagę przez sądy. W granicach prawa, inne elementy, takie jak zwyczaje, regulaminy, kodeksy etyki, umowy oraz ogólny kontekst oraz okoliczności sprawy, mogą być także wzięte pod uwagę, jeżeli określają, czy dany cel jest uzasadniony. Będzie to obejmować charakter relacji pomiędzy administratorem oraz osobami, których dane dotyczą, czy to handlowych czy innych”. Dalej, to co może być uznane za uzasadniony interes „może się także zmienić z czasem, w zależności od naukowego oraz technologicznego rozwoju, oraz zmian w postawach społecznych oraz kulturowych”.

[49] Kwestia technologii śledzących oraz rola zgody zgodnie z art. 5 ust. 3) dyrektywy o prywatności i łączności elektronicznej będzie przedyskutowana oddzielnie. Zobacz część III.3.6 b) pod tytułem: *„Przykład: ewolucja podejścia do marketingu bezpośredniego”*

[50] Zobacz Część 4.2.3 Opinii już cytowanej w przypisie 39 powyżej. Uzasadniony interes administratora w tej sprawie był także połączony z interesem publicznym kraju trzeciego, który nie może być zastosowany zgodnie z dyrektywą 95/46/WE.

na art. 7 lit. f). Grupa Robocza uważa w szczególności, że z powodu daleko idących skutków dla jednostek, przetwarzania danych w ‘sposób ukryty, systematyczny, masowy lub długotrwały’ ‘interesy związane z prawami podstawowymi i wolnościami dużej liczby osób, których dane dotyczą, są nadrzędne wobec interesu SWIFT, aby nie być objętym sankcjami przez USA za ewentualny brak zgodności z pozwami’.

Jak zostanie wykazane później, jeżeli interes administratora nie jest istotny, interesy oraz prawa osób, których dane dotyczą, będą z większym prawdopodobieństwem nadrzędne wobec prawnie uzasadnionego – lecz mniej znaczącego – interesu administratora. Równocześnie nie oznacza to, że mniej ważne interesy administratora nie mogą czasem być nadrzędne wobec interesów oraz praw osób, których dane dotyczą: zdarza się to zwykle, gdy wpływ przetwarzania na osoby, których dane dotyczą jest mniej znaczący.

Prawnie uzasadniony interes w sektorze publicznym

Obecny tekst dyrektywy nie wyklucza szczegółowo administratorów będących organami publicznymi z przetwarzania danych przy wykorzystaniu art. 7 lit. f) jako podstawy prawnej.[51]

Jednakże proponowane rozporządzenie[52] wyklucza taką możliwość odnośnie „przetwarzania realizowanego przez organy publiczne w wykonaniu ich zadań.

Proponowana zmiana legislacyjna podkreśla znaczenie ogólnej zasady, że organy publiczne, co do zasady, powinny przetwarzać dane w wykonaniu ich zadań tylko, jeżeli są odpowiednio upoważnione przez prawo, aby to uczynić. Zgodność z tą zasadą jest szczególnie istotna – oraz jasno wymagana przez orzecznictwo Europejskiego Trybunału Praw Człowieka – w przypadkach, gdzie dotyczy to kwestii prywatności osób, których dane dotyczą a działalność organów publicznych naruszałaby tą prywatność.

Wystarczająco szczegółowe oraz konkretne upoważnienie przez prawo jest z tego względu wymagane – także na podstawie obecnej dyrektywy – w przypadku gdy przetwarzanie przez organy publiczne narusza prywatność osób, których dane dotyczą. Może to przyjąć albo formę konkretnego obowiązku prawnego do przetwarzania danych, który może wypełnić przesłanki art. 7 lit. c), lub konkretnego upoważnienia (choć niekoniecznie obowiązku) do przetwarzania danych, które może spełnić wymagania art. 7 lit. e) lub f).[53]

Prawnie uzasadnione interesy osób trzecich

[51] Pierwotnie, pierwszy wniosek Komisji dotyczący dyrektywy obejmował odrębnie przetwarzanie danych w sektorze prywatnym oraz czynności przetwarzania w sektorze publicznym. To formalne rozróżnienie pomiędzy regułami stosującymi się do sektora publicznego oraz prywatnego zostało porzucone w poprawionej wersji. To mogło także doprowadzić do różnic w interpretacji oraz wdrożeniu przez różne państwa członkowskie.

[52] Zobacz art. 6 ust. 1 lit. f) proponowanego Rozporządzenia

[53] W tym aspekcie, zobacz także Część III.2.5. powyżej na temat zadań publicznych (strony 21-23) jak również dyskusję poniżej pod tytułem *Prawnie uzasadnione interesy osób trzecich* (na stronach 27-28). Zobacz także rozważania na temat ograniczeń „prywatnego wdrażania” prawa na stronie 35 pod tytułem „Interes publiczny/ interes szerszej społeczności”. We wszystkich tych sytuacjach jest szczególnie istotne, aby zapewnić, że granice art. 7 lit. f) oraz 7 lit. e) są w pełni szanowane.

Obecny tekst dyrektywy nie tylko odnosi się do „prawnie uzasadnionych interesów administratora", ale także pozwala na wykorzystanie art. 7 lit. f), w przypadku „prawnie uzasadnionych interesów osoby trzeciej, lub osób, którym dane są ujawniane"[54]. Następne przykłady zilustrują niektóre z kontekstów, gdzie przepis ten może mieć zastosowanie.

Publikowanie danych dla celów przejrzystości oraz rozliczalności. Jednym z istotnych kontekstów, gdzie art. 7 lit. f) może być odpowiedni, jest przypadek publikacji danych dla celów przejrzystości oraz rozliczalności (na przykład wynagrodzenie wyższej kadry kierowniczej w firmie). W tym przypadku można uznać, że publiczne ujawnienie jest wykonane w pierwszym rzędzie nie w interesie administratora, który publikuje dane, lecz raczej, w interesie innych zainteresowanych osób, takich jak pracownicy lub dziennikarze, lub opinia publiczna, którym dane są ujawniane.

Z perspektywy ochrony danych oraz prywatności, oraz aby zapewnić pewność prawną, generalnie zaleca się, aby dane osobowe były udostępnianie publicznie na podstawie prawa pozwalającego oraz – gdzie to odpowiednie – jasno określającego dane, które mają być opublikowane, cele publikacji oraz konieczne środki ochronne.[55] Oznacza to także, że może być właściwsze wykorzystanie raczej art. 7 lit. c) niż 7 lit. f) jako podstawy prawnej, kiedy dane są publikowane dla celów przejrzystości oraz rozliczalności.[56]

Jednakże w przypadku braku konkretnego obowiązku prawnego lub zezwolenia na publikację danych byłoby i tak możliwe ujawnienie danych osobowych zainteresowanym osobom. W odpowiednich przypadkach możliwe byłoby także opublikowanie danych osobowych dla celów przejrzystości oraz rozliczalności.

W obu przypadkach – tj. niezależnie od tego, czy dane osobowe są ujawniane na podstawie prawa na to pozwalającego czy nie – ujawnienie zależy bezpośrednio od wyników testu równowagi art. 7 lit. f) oraz od wdrożenia odpowiednich zabezpieczeń oraz środków.[57]

---

[54] Celem proponowanego Rozporządzenia jest ograniczenie wykorzystania tej podstawy do „prawnie uzasadnionych interesów administratora. Nie jest jasne z samego tekstu czy proponowany język oznacza po prostu ułatwienie teksty czy jego intencją jest wykluczenie sytuacji, gdzie administrator mógłby ujawnić dane w uzasadnionym interesie innych. Ten tekst nie jest jednakże ostateczny. Interes osób trzecich został na przykład ponownie umieszczony w Ostatecznym Sprawozdaniu Komisji LIBE z okazji głosowania nad kompromisowymi poprawkami Komisji LIBE Parlamentu Europejskiej z 21 października 2013 r. Zobacz poprawkę 100 do art. 6. Ponowne wprowadzenie osób trzecich do propozycji jest wspierane przez Grupę Roboczą na tej podstawie, że wykorzystanie tego przepisu może być odpowiednie w niektórych sytuacjach, włączając w nie te opisane poniżej.

[55] Te zalecenia w zakresie dobrych praktyk nie powinny być z uszczerbkiem dla krajowych reguł prawnych na temat przejrzystości oraz publicznego dostępu do dokumentów.

[56] Istotnie, w niektórych państwach członkowskich należy zachować zgodność z różnymi regułami w odniesieniu do przetwarzania przez podmioty publiczne i prywatne. Na przykład, zgodnie z włoską ustawą o ochronie danych rozpowszechnianiu danych osobowych przez podmioty publiczne może być dozwolone tylko, jeżeli taka możliwość jest przewidziana przez prawo lub rozporządzenia (Część 19.3).

[57] Jak wyjaśniono w Opinii Grupy Roboczej 06/2013 w sprawie otwartych danych (zobacz strona 9 opinii, cytowana w przypisie 88 poniżej), każde krajowe działanie lub przepisy prawa w odniesieniu do przejrzystości muszą być zgodne z art. 8 Europejskiej Konwencji Praw Człowieka oraz art. 7 oraz 8 Karty Praw Podstawowych. Oznacza to, iż zgodnie z orzeczeniem Europejskiego Trybunału Sprawiedliwości w sprawie Österreichischer Rundfunk i Schecke, należy ustalić, że ujawnienie jest konieczne i proporcjonalne do celu zgodnego z prawem, do którego dąży się w ramach przepisów. Zobacz TS UE 20 maja 2003, Rundfunk, połączone sprawy C-465/00,

Dodatkowo dalsze wykorzystanie dla większej przejrzystości już ujawnionych danych osobowych (na przykład ponowna publikacja danych przez prasę lub dalsze rozpowszechnienie pierwotnie opublikowanego zbioru w bardziej innowacyjny oraz przyjazny użytkownikowi sposób przez organizacje pozarządowe) może także być pożądane. To czy taka ponowna publikacja oraz ponowne wykorzystanie jest możliwe, będzie także zależeć od rezultatu testu równowagi, przy którym powinno się brać pod uwagę, między innymi, charakter informacji oraz skutek ponownej publikacji oraz ponownego wykorzystania dla osób.[58]

Badania historyczne oraz innego rodzaju badania naukowe. Następnym ważnym kontekstem, w którym ujawnienie może być właściwe biorąc pod uwagę interes stron trzecich, są badania historyczne lub inne rodzaje badań naukowych, w szczególności gdy wymagany jest dostęp do niektórych zbiorów. Dyrektywa zapewnia uznanie tego typu działań, przy zastosowaniu odpowiednich zabezpieczeń oraz środków[59], jednakże nie należy zapominać, że prawnie uzasadnioną podstawą dla tych działań często będzie uważnie przemyślane wykorzystanie art. 7 lit. f).[60]

Ogólny interes publiczny lub interes osoby trzeciej. Na koniec, prawnie uzasadniony interes osób trzecich, może znajdować zastosowanie także w inny sposób. Jest to przypadek, w którym interes administratora – czasem zachęconego przez organy publiczne – odpowiada ogólnemu interesowi publicznemu lub interesowi osoby trzeciej. Może to obejmować sytuacje, w których administrator wykracza poza konkretne zobowiązania ustanowione przez ustawy i rozporządzania, aby pomóc organom ds. egzekwowania prawa lub prywatnym zainteresowanym osobom, w ich wysiłkach w zwalczaniu nielegalnych działań, takich jak pranie pieniędzy, nagabywania dzieci, lub nielegalne dzielenie się plikami w Internecie. Jednakże w tych sytuacjach, szczególnie istotne jest zapewnienie, że granice art. 7 lit. f) są całkowicie szanowane.[61]

Przetwarzanie musi być konieczne dla zamierzonych celów

C-138/01 oraz 139/01 oraz TS UE 9 listopada 20130, Volker und Markus Schecke, połączone sprawy C-92/09 oraz C-93/09.

[58] Ograniczenie celu jest także tutaj ważne. Na stronie 19 opinii Grupy Roboczej 06/2013 na temat otwartych danych (zacytowanej w przypisie 88 poniżej, GR Art. 29 „zaleca, by przepisy przewidujące publiczny dostęp do danych jasno określały cele udostępniania danych osobowych. Jeżeli tak się nie stanie albo cele te będą określone w sposób nieprecyzyjny i szeroki, ucierpi na tym pewność i przewidywalność prawa. W szczególności w odniesieniu do każdego wniosku o ponowne wykorzystanie danych organowi sektora publicznego i odnośnym, potencjalnym ponownym użytkownikom będzie bardzo trudno ustalić, jakie były zamierzone pierwotne cele upublicznienia, a tym samym, jakie dalsze cele byłyby zgodne z tymi pierwotnymi celami. Jak już wspomniano, nawet jeżeli dane osobowe zostały opublikowane w Internecie, nie należy zakładać, że można je dalej przetwarzać w jakichkolwiek możliwych celach.

[59] Zobacz na przykład art. 6 ust. 1 lit. b) oraz e)

[60] Jak wyjaśniono w opinii 3/2013 Grupy Roboczej w sprawie ograniczenia celu (cytowanej w przypisie 9 powyżej), dalsze wykorzystanie danych dla wtórnych celów musi być przedmiotem podwójnego testu. Po pierwsze, powinno się zapewnić, ze dane będą przetwarzane w zgodnych celach. Po drugie powinno się zapewnić, że będzie odpowiednia podstawa prawna przetwarzania zgodnie z art. 7.

[61] Zobacz w tym względzie na przykład dokument roboczy dotyczący kwestii danych związanych z prawami własności intelektualnej, przyjęty 19.I.2005 r. (WP104).

Na koniec, przetwarzanie danych osobowych musi być również ‘konieczne dla potrzeb wynikających z uzasadnionych interesów’ administratora danych lub – w przypadku ujawnienia – osób trzecich. Warunek ten uzupełnia wymóg konieczności zgodnie z art. 6 oraz wymaga połączenia pomiędzy przetwarzaniem oraz interesem. Ten wymóg „konieczności” znajduje zastosowanie we wszystkich sytuacjach wspomnianych w art. 7, litery b) do f), jednak jest szczególnie istotny w kontekście litery f), aby zapewnić, że przetwarzanie danych oparte na prawnie uzasadnionym interesie nie będzie prowadzić do nadmiernie szerokiej interpretacji konieczności przetwarzania danych. Tak jak w innych przypadkach, oznacza to, że należy rozważyć, czy nie są dostępne mniej inwazyjne środki, służące temu samemu celowi.

III.3.2. Interesy lub prawa osoby, której dane dotyczą

Interesy lub prawa (a nie interesy związane z podstawowymi prawami)

W art. 7 lit. f) dyrektywy napisano „interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1.”

Grupa Robocza jednakże zauważyła, porównując różne wersje językowe dyrektywy, że zwrot „interesom związanym” został przetłumaczony „interesom lub” w innych kluczowych językach, które były używane w momencie, kiedy tekst był negocjowany.[62]

Dalsza analiza wskazuje, że angielski tekst dyrektywy jest po prostu wynikiem pominięcia litery: „or” zostało błędnie wpisane jako „for”[63]. Z tego względu prawidłowy tekst powinien brzmieć „interesy lub podstawowe prawa i wolności”.

„Interesom” oraz „prawom” należy nadać szeroką interpretację

Odniesienie do „interesów lub podstawowych praw i wolności” ma bezpośredni wpływ na zakres zastosowania przepisu. Zapewnia większą ochronę osobie, której dane dotyczą, mianowicie wymaga, aby również „interesy” osób, których dane dotyczą, były brane pod uwagę, nie tylko jej lub jego prawa i podstawowe wolności. Jednakże nie ma powodu, aby zakładać, że ograniczenie art. 7 lit. f) do podstawowych praw „które wymagają ochrony zgodnie z art. 1 ust. 1) – i w ten sposób, wyraźne odwołanie do przedmiotu dyrektywy[64] – nie

[62] Na przykład 'l'intérêt ou les droits et libertés fondamentaux de la personne concernée' po francusku, 'l'interesse o i diritti e le libertà fondamentali della persona interessata' po włosku; 'das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person' po niemiecku.

[63] Grupa Robocza zauważa, że gramatycznie poprawna wersja angielska powinna brzmieć „interests in” a nie „interests for”, jeżeli to miano na myśli. Ponadto zwrot „interests for” lub „interests in” wydaje się po pierwsze zbędny, ponieważ odwołanie do „podstawowych praw oraz wolności” zwykle wystarcza, jeżeli to miano na myśli. Interpretacja, że doszło do błędu literowego jest także potwierdzona przez okoliczność, że wspólne stanowisko (WE) Nr 1/95, przyjęte przez Radę 20 lutego 1995 r. także odnosi się do „interesów lub podstawowych praw i wolności”. Na końcu należy wspomnieć, że Grupa Robocza zauważa także, że Komisja zamierzała poprawić ten błąd literowy w proponowanym Rozporządzeniu: Art. 6 ust. 1 lit. f) odnosi się do „interesów lub podstawowych praw i wolności osoby, której dane dotyczą, które wymają ochrony danych osobowych”, a nie interesów „związanych” z takimi prawami.

[64] Zobacz art. 1 ust. 1 „Zgodnie z przepisami niniejszej dyrektywy, państwa członkowskie zobowiązują się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych.”

miałoby także zastosowania do pojęcia „interesy”. Jasnym przekazem jest jednakże to, że wszystkie właściwe interesy osoby, której dane dotyczą, powinny być wzięte pod uwagę.

(Taka) interpretacja jest nie tylko sensowna pod względem gramatycznym, ale także kiedy bierze się pod uwagę szeroką interpretację pojęcia ‘prawnie uzasadnionych interesów administratora’. Jeżeli administrator – lub osoba trzecia w przypadku ujawnienia – posiada interesy, zakładając, że nie są nieuzasadnione, wówczas osoba, której dane dotyczą powinna także mieć prawo do tego, aby wszystkie kategorie jej interesów także były brane pod uwagę, oraz aby były wyważane względem interesów administratora, tak długo jak są istotne biorąc pod uwagę zakres dyrektywy.

W czasach wzrastającej nierównowagi „potęgi informacyjnej”, gdy rządy oraz organizacje biznesowe gromadzą dotychczas bezprecedensową liczbę danych na temat jednostek, oraz są w stanie coraz bardziej zestawiać szczegółowe profile, na podstawie których można przewidzieć ich zachowanie (wzmacnianie nierównowagi informacyjnej oraz zmniejszanie ich autonomii), jest nawet bardziej istotne, aby zapewnić, że interesy osób do zabezpieczenia ich prywatności oraz autonomii są chronione.

Na koniec, ważne jest, aby zauważyć, że inaczej niż w przypadku interesów administratora, przymiotnik „prawnie uzasadniony” nie jest umieszczony przed pojęciem „interesów” osoby której dane dotyczą. Powoduje to szerszy zakres ochrony interesów oraz praw osób. Nawet osoby zaangażowane w nielegalne działalności nie powinny stać się przedmiotem nieproporcjonalnego naruszenia ich praw oraz interesów.[65] Na przykład, interesy osoby, która dokonała kradzieży w supermarkecie, ciągle mogą być nadrzędne wobec publikacji jej zdjęcia oraz prywatnego adresu na ścianach supermarketu oraz/lub w Internecie, przez właściciela sklepu.

III.3.3. Wprowadzenie do stosowania testu równowagi

Użyteczne jest wyobrażenie sobie zarówno prawnie uzasadnionych interesów administratora, jak i wpływu na interesy oraz prawa osoby, której dane dotyczą, w szerokim kontekście. Prawnie uzasadnione interesy mogą sięgać od nieistotnych, poprzez dość znaczące aż po istotne. Podobnie wpływ na interesy oraz prawa osób, których dane dotyczą, może być bardziej lub mniej znaczący oraz może sięgać od błahego po bardzo poważny.

Prawnie uzasadnione interesy administratora, gdy są drobne i niezbyt istotne, mogą generalnie być nadrzędne wobec interesów oraz praw osób, których dane dotyczą, w przypadkach, gdy wpływ na te prawa oraz interesy jest jeszcze bardziej błahy. Z drugiej strony ważny oraz istotny prawnie uzasadniony interes może w niektórych przypadkach oraz przy zastosowaniu odpowiednich zabezpieczeń oraz środków uzasadnić nawet znaczące naruszenie prywatności lub inny znaczący wpływ na interesy oraz prawa osób, których dane dotyczą[66].

[65] Oczywiście jedną z konsekwencji przestępczości może być zbieranie oraz możliwa publikacja danych osobowych na temat przestępców oraz podejrzanych. Jednakże musi to być podlegać ścisłym warunkom oraz zabezpieczeniom.

[66] Patrz: rozumowanie Grupy Roboczej przedstawione w kilku opiniach i dokumentach roboczych:

- Opinia 4/2006 w sprawie Powiadomienia dotyczącego wniosku legislacyjnego Departamentu Zdrowia i Opieki Społecznej Stanów Zjednoczonych w sprawie kontroli chorób zakaźnych i zbierania informacji o pasażerach

Istotne jest tutaj, aby podkreślić szczególną rolę, jaką mają do odegrania zabezpieczenia[67] w zmniejszaniu nadmiernego wpływu na osoby, których dane dotyczą i w ten sposób w zmienianiu równowagi praw oraz interesów tak, aby prawnie uzasadnione interesy administratora danych nie stały się podrzędne. Samo wykorzystanie zabezpieczeń nie jest oczywiście wystarczające, aby uzasadnić jakikolwiek typ przetwarzania we wszystkich kontekstach. Ponadto, omawiane zabezpieczenia muszą być odpowiednie oraz wystarczające i muszą niekwestionowanie oraz znacząco zmniejszyć wpływ na osoby, których dane dotyczą.

Scenariusze wprowadzające

Przed przejściem do wskazówek na temat tego, jak przeprowadzać test równowagi, trzy poniższe scenariusze mogą wstępnie zobrazować, jak równoważenie interesów oraz praw może wyglądać w praktyce. Wszystkie trzy przykłady biorą swój początek w prostym oraz niewinnym scenariuszu, rozpoczynającym się od specjalnej oferty włoskiej restauracji specjalizującej się w jedzeniu na wynos. Przykłady stopniowo wprowadzają nowe elementy, które pokazują jak równowaga jest przechylona, kiedy wpływ na osoby, których dane dotyczą wzrasta.

Scenariusz 1: specjalna oferta sieci pizzerii

Claudia zamawia pizzę poprzez aplikację mobilną na swoim smartfonie, jednak nie zaznacza opcji opt-out w odniesieniu do marketingu na stronie internetowej. Jej adres oraz szczegóły karty bankowej są przechowywane dla celów dostawy. Kilka dni później Claudia otrzymuje kupony rabatowe na podobne produkty sieci pizzerii na swoją domową skrzynkę pocztową.

Krótka analiza: sieć pizzerii ma prawnie uzasadniony, ale nie szczególnie istotny interes w próbie sprzedaży większej ilości produktów swoim klientom. Z drugiej strony nie wydaje się, aby doszło do jakiegokolwiek poważnego naruszenia prywatności Claudii, ani innego nadmiernego wpływu na jej interesy oraz prawa. Dane oraz kontekst są względnie niewinne (konsumpcja pizzy). Sieć pizzerii ustanowiła pewne zabezpieczenia: wykorzystywane są jedynie względnie ograniczone informacje (dane kontaktowe), a kupony są przesyłane pocztą tradycyjną. Dodatkowo zapewniono łatwą do wykorzystania opcję opt-out na stronie internetowej w odniesieniu do marketingu.

Porównując oraz biorąc pod uwagę ustanowione zabezpieczenia oraz środki (w tym łatwy do wykorzystania mechanizm opt-out), interesy oraz prawa osoby, której dane dotyczą nie

z dnia 20 listopada 2005 r. (Wniosek w sprawie kontroli chorób zakaźnych 42 CFR część 70 i 71), przyjęta 14 czerwca 2006 r. (WP 121), gdzie mowa jest o konkretnych poważnych zagrożeniach zdrowia publicznego.
- Opinia 1/2006 w sprawie systemów informowania o nieprawidłowościach (cytowanej w przypisie 39), gdzie waga rzekomego przestępstwa jest jednym z elementów testu równowagi.
- Dokument roboczy w sprawie nadzoru komunikacji elektronicznej w miejscu pracy, przyjęty 29.05.2002 r. (WP 55), który wyważa prawo pracownika do efektywnego prowadzenia działalności względem godności ludzkiej pracownika, jak również poufności korespondencji.

[67] Zabezpieczania mogą obejmować m.in. restrykcyjne ograniczenia odnośnie do ilości danych, które można gromadzić, natychmiastowe usuwanie danych po wykorzystaniu, środki techniczne i organizacyjne w celu zapewnienia oddzielenia funkcjonalnego, odpowiednie wykorzystywanie technik anonimizacji, łączenie danych oraz technologie służące zwiększaniu ochrony prywatności, ale również zwiększona przejrzystość, rozliczalność oraz możliwość wycofania zgody na przetwarzanie (tzw. opt-out). Patrz także Część III.3.4(d) poniżej.

wydają się być nadrzędne wobec prawnie uzasadnionego interesem sieci pizzerii do przeprowadzenia tej minimalnej operacji przetwarzania danych.

Scenariusz 2: ukierunkowana reklama dla tej samej specjalnej oferty

Kontekst jest taki sam, ale tym razem nie tylko adres Claudii oraz szczegóły karty kredytowej, ale także jej historia ostatnich zamówień (za okres trzech lat) jest przechowywana przez sieć pizzerii. Dodatkowo historia zakupów jest zestawiana z danymi z supermarketu, gdzie Claudia robi zakupy internetowe, który jest zarządzany przez tę samą firmę, która kieruje siecią pizzerii. Sieć pizzerii przesyła Claudii specjalne oferty oraz ukierunkowaną reklamę opartą na jej historii zakupów dla dwóch różnych usług. Otrzymuje reklamy oraz specjalne oferty zarówno przez Internet, jak i poza nim, przez zwykłą pocztę, pocztę elektroniczną, umieszczanie na stronie internetowej firmy, jak również na stronach internetowych wybranych partnerów (kiedy wchodzi ona na te strony przez swój komputer lub przez swój telefon komórkowy). Jej historia wyszukiwania (click-stream) jest również śledzona. Jej dane lokalizacyjne są również śledzone przez jej telefon komórkowy. Oprogramowanie typu analytics analizuje dane i przewiduje jej preferencje, a także czas oraz lokalizacje, w których jest najbardziej prawdopodobne to, że będzie dokonywać dużych zakupów, że będzie skłonna zapłacić wyższą cenę, że będzie podatna na konkretną wielkość obniżki cen lub kiedy będzie miała największą ochotę na swój ulubiony deser lub gotowy posiłek[68]. Claudia jest dogłębnie zirytowana przez nieustanne reklamy wyskakujące na jej telefonie komórkowym, kiedy sprawdza rozkład jazdy autobusów wracając do domu, reklamujące ostatnie oferty jedzenia na wynos, którym stara się oprzeć. Nie była w stanie znaleźć przyjaznej użytkownikowi informacji lub prostej drogi do wyłączenia tych reklam, chociaż firma utrzymuje, że istnieje sektorowy mechanizm opt-out. Była także zdziwiona, że gdy przeprowadziła się do mniej zamożnej dzielnicy, to nie otrzymywała więcej specjalnych ofert. Poskutkowało to zwiększeniem jej miesięcznych wydatków na jedzenie o koło 10%. Bardziej uzdolniony technicznie przyjaciel pokazał jej na blogu internetowym informacje na temat określonych spekulacji polegających na tym, że supermarket pobierał większe opłaty za zamówienia ze „złych dzielnic", na podstawie statystycznie wyższego ryzyka oszustw związanych z kartami kredytowymi w takich przypadkach. Firma nie skomentowała tego oraz utrzymuje, że jej polityka dotycząca obniżek oraz algorytm, który wykorzystuje do ustalania cen, jest jej własnością i nie może być ujawniony.

Krótka analiza: charakter danych oraz kontekstu pozostaje względnie niewinny. Jednakże skala zbierania danych oraz techniki wykorzystane do wpłynięcia na Claudię (w tym różne mechanizmy śledzenia, przewidywanie czasu oraz lokalizacji chęci na jedzenie oraz okoliczność, że w tym czasie Claudia jest bardziej podatna na ulegnięcie pokusie), są czynnikami, które należy rozważyć przy ocenie wpływu przetwarzania. Brak przejrzystości na temat logiki przetwarzania danych przez firmę, która mogła de facto doprowadzić do dyskryminacji cenowej opartej na lokalizacji zamówienia, oraz potencjalny znaczący wpływ

[68] Patrz np. http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards: *'Ostatnie badanie sugeruje, że siła woli jest ograniczonym źródłem, które z czasem może być uszczuplone lub uzupełnione.[10]Wyobraź sobie, że obawy przed otyłością prowadzą konsumentkę do próby powstrzymania się przed jedzeniem jej ulubionego śmieciowego jedzenia. Okazuje się, że istnieją takie terminy i miejsca, gdy nie może tego robić. Big data mogą pomóc sprzedawcom dokładnie zrozumieć, jak i kiedy zwrócić się do tej konsumentki, gdy jest najbardziej podatna – szczególnie w świecie ciągłego czasu antenowego, w którym nawet nasze urządzenia są celem oferty sprzedażowej'.*

finansowy na klientów, ostatecznie doprowadza do zachwiania równowagi nawet we względnie niewinnym kontekście jedzenia na wynos oraz zakupów spożywczych. Zamiast oferować jedynie możliwość zastosowania mechanizmu opt-out odnośnie tego typu profilowania oraz ukierunkowanej reklamy, świadoma zgoda byłaby konieczna, zgodnie z art. 7 lit. a) ale także zgodnie z art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. W rezultacie art. 7 lit. f) nie powinien być podstawą prawną takiego przetwarzania.

Scenariusz 3: wykorzystanie zamówień jedzenia do dostosowania składek ubezpieczenia zdrowotnego

Nawyki jedzenia pizzy przez Claudię, w tym czas oraz charakter zamówień jedzenia, są sprzedawane przez sieć firmie ubezpieczeniowej, która wykorzystuje je do dostosowania składek ubezpieczenia zdrowotnego.

Krótka analiza: firma zajmująca się ubezpieczeniami zdrowotnymi może mieć prawnie uzasadniony interes – w zakresie w jakim pozwalają na to właściwe regulacje – w zakresie oceny ryzyka zdrowotnego swoich klientów i proponować zróżnicowane oferty do różnych ryzyk. Jednakże sposób, w jaki dane są zbierane, oraz skala zbierania danych same w sobie są nadmierne. Racjonalna osoba w sytuacji Claudii raczej nie oczekiwałaby, że jej informacje na temat konsumpcji pizzy byłyby używane do obliczania ofert ubezpieczenia zdrowotnego.

Dodatkowo do nadmiernego charakteru profilowania oraz możliwych niedokładnych wniosków (pizza mogłaby być zamówiona przez kogoś innego), wnioskowanie na temat danych wrażliwych (danych o zdrowiu) z wydawałoby się nieszkodliwych danych (zamówienie żywności na wynos) przyczynia się do zachwiania równowagi na korzyść interesów oraz praw osoby, której dane dotyczą. Na koniec, przetwarzanie ma także znaczący wpływ finansowy na nią.

Wyważając te kwestie, w tym konkretnym przypadku interesy oraz prawa osoby, które dane dotyczą, są nadrzędne wobec prawnie uzasadnionego interesu firmy zajmującej się ubezpieczeniami zdrowotnymi. W rezultacie art. 7 nie powinien być podstawą prawną przetwarzania. Wątpliwe jest także, czy art. 7 lit. a) mógłby być wykorzystany jako podstawa prawna, biorąc pod uwagę nadmierną skalę zbierania danych, oraz być może także w związku z dalszymi konkretnymi ograniczeniami wynikającymi z prawa krajowego.

Powyższe scenariusze oraz możliwe wprowadzenie zmian z innymi elementami podkreślają potrzebę ograniczonej liczby kluczowych czynników, które mogą pomóc zogniskować ocenę, jak również potrzebę pragmatycznego podejścia, które pozwala na wykorzystanie praktycznych założeń (‘zasada kciuka), opartych w pierwszym rzędzie na tym, co rozsądna osoba uznałaby za do przyjęcia w danych okolicznościach (‘rozsądne oczekiwania’) oraz opierając się na konsekwencjach czynności przetwarzania danych dla osób, których dane dotyczą (‘wpływ’).

III.3.4. Kluczowe czynniki, które należy uwzględnić przy stosowaniu testu równowagi

Państwa członkowskie określiły dużą liczbę użytecznych czynników, które należy rozważyć przy przeprowadzaniu testu równowagi. Czynniki te są omówione w tej części pod następującymi czterema głównymi tytułami: a) ocena prawnie uzasadnionego interesu

administratora, b) wpływ na osoby, których dane dotyczą, c) tymczasowa równowaga oraz d) dodatkowe zabezpieczenia zastosowane przez administratora do zapobiegania nadmiernemu wpływowi na osoby, których dane dotyczą[69].

Aby przeprowadzić test równowagi ważne jest, aby rozważyć charakter oraz źródło uzasadnionego interesu z jednej strony oraz wpływ na osoby, których dane dotyczą, z drugiej. Ocena ta powinna już brać pod uwagę środki, które administrator planuje przyjąć w celu zapewnienia zgodności z dyrektywą (na przykład, aby zapewnić ograniczenie celu oraz proporcjonalność, zgodnie z art. 6, lub aby zapewnić informacje osobom, których dane dotyczą, zgodnie z art. 10 oraz 11).

Po przeanalizowaniu oraz wyważeniu tych dwóch stron względem siebie, może być zastosowana tymczasowa „równowaga". Gdy rezultat oceny ciągle pozostawia wątpliwości, następnym krokiem byłaby ocena, czy dodatkowe zabezpieczenia, zapewniające więcej ochrony osobom, których dane dotyczą, mogą zmienić równowagę w taki sposób, aby uprawomocnić przetwarzanie.

a) Ocena prawnie uzasadnionego interesu administratora

Podczas gdy pojęcie prawnie uzasadnionego interesu jest dość szerokie, jak to wyjaśniono w Części III.3.1. powyżej, jego charakter odgrywa kluczową rolę, kiedy dochodzi do wyważenia interesów względem praw oraz interesów osób, których dane dotyczą. Chociaż nie jest możliwe dokonanie ocen wartości w odniesieniu do wszystkich możliwych prawnie uzasadnionych interesów, możliwe jest zapewnienie pewnych wytycznych. Jak wspomniano wyżej, taki interes może sięgać od błahego po istotny, oraz może być prosty lub bardziej kontrowersyjny.

i) Realizacja praw podstawowych

Spośród podstawowych praw oraz wolności zapisanych w Europejskiej Karcie Praw Podstawowych (zwanej 'Kartą')[70] oraz Europejskiej Konwencji Praw Człowieka ('EKPCz'), kilka może wejść w konflikt z prawem do prywatności oraz prawem ochrony danych osobowych, takim jak np. wolność wypowiedzi i informacji[71], wolność sztuk i nauk[72], prawo dostępu do dokumentów[73], jak również na przykład prawo do wolności oraz bezpieczeństwa[74], wolność myśli, sumienia oraz wyznania[75], wolność prowadzenia działalności gospodarczej[76], prawo własności[77], prawo do skutecznych środków ochrony prawnej oraz uczciwego procesu[78], lub domniemanie niewinności oraz prawo do obrony[79].

[69] Ze względu na ich wagę, niektóre konkretne kwestie dotyczące środków zabezpieczeń zostaną dalej omówione w odrębnych nagłówkach w Częściach III.3.5 oraz III.3.6.

[70] Przepisy Karty skierowane są do instytucji i organów UE z należytym uwzględnieniem zasady pomocniczości oraz do krajowych organów, tylko jeżeli wdrażają prawo UE.

[71] Artykuł 11 Karty oraz artykuł 10 EKPCz (Europejskiej Konwencji Praw Człowieka).

[72] Artykuł 13 Karty oraz artykuły 9 i 10 EKPCz.

[73] Artykuł 42 Karty. 'Każdy obywatel Unii i każda osoba fizyczna lub prawna mająca miejsce zamieszkania lub statutową siedzibę w Państwie Członkowskim ma prawo dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji'. Podobne prawa dostępu istnieją w szeregu państw członkowskich w odniesieniu do dokumentów będących w posiadaniu organów publicznych w tych państwach członkowskich.

[74] Artykuł 6 Karty oraz artykuł 5 EKPCz.

[75] Artykuł 10 Karty oraz artykuł 9 EKPCz.

[76] Artykuł 16 Karty.

Aby prawnie uzasadniony interes administratora był nadrzędny, przetwarzanie danych musi być „konieczne" oraz „proporcjonalne" do realizacji określonego prawa podstawowego.

Aby zobrazować tę kwestię, w zależności od danej sytuacji, może być „konieczne" oraz „proporcjonalne", aby gazeta opublikowała pewne obciążające szczegóły na temat zwyczajów wydawania pieniędzy przez wysoko postawionych urzędników rządowych, zaangażowanych w domniemany skandal korupcyjny. Z drugiej strony, nie powinno być blankietowego pozwolenia dla mediów na publikację wszystkich nieistotnych szczegółów prywatnego życia osób publicznych. Takie oraz podobne sprawy zwykle powodują konieczność rozważenia wielu kwestii, a istotną rolę pomagającą w ocenie mogą odegrać: konkretne prawo, orzecznictwo, prawoznawstwo, wytyczne, jak również regulaminy lub bardziej lub mniej formalne standardy[80].

Gdy to właściwe, także w tym kontekście, dodatkowe zabezpieczenia mogą odegrać ważną rolę oraz pomóc określić, w jaki sposób osiągnąć- czasem chwiejną – równowagę.

ii) Interesy publiczne/ interesy szerszej społeczności

W niektórych przypadkach administrator może chcieć przywołać interes publiczny lub interes szerszej społeczności (niezależnie od tego, czy istnieje taki przepis w ustawach czy rozporządzeniach krajowych). Na przykład organizacja charytatywna może przetwarzać dane osobowe dla celów badań medycznych, lub organizacja non-profit może przetwarzać dane w celu zwiększenia świadomości na temat korupcji w rządzie.

Może się także zdarzyć sytuacja, że prywatny interes biznesowy firmy współgra do pewnego stopnia z interesem publicznym. Może mieć to miejsce, na przykład, w odniesieniu do zwalczania przestępstw finansowych lub innego niezgodnego z prawem wykorzystywania usług[81]. Dostawca usług może mieć prawnie uzasadniony interes biznesowy w zapewnieniu tego, że jego klienci nie wykorzystują usług niezgodnie z przeznaczeniem (lub że nie będą w stanie otrzymać dostępu do usług bez płatności), podczas gdy w tym samym czasie klienci firmy, podatnicy oraz ogólnie opinia publiczna także mają prawnie uzasadniony interes w zapewnieniu, że zniechęca się do niezgodnych z prawem działań, a także je wykrywa.

Ogólnie okoliczność, że administrator działa nie tylko w swoim prawnie uzasadnionym (biznesowym) interesie, ale także w interesie szerszej społeczności, może dodać więcej

---

[77] Artykuł 17 Karty oraz artykuł 1 Protokołu nr do EKPCz.

[78] Artykuł 47 karty oraz artykuł 6 EKPCz.

[79] Artykuł 48 Karty oraz artykuły 6 i 13 EKPCz.

[80] W odniesieniu do kryteriów, które należy stosować w przypadkach obejmujących wolność wypowiedzi, orzecznictwo Europejskiego Trybunału Praw Człowieka również zapewnia przydatne wytyczne. Patrz np. wyrok ETPCz w sprawie von Hannover v Germany (nr 2) z 7 lutego 2012 r., w szczególności ust. 95-126. Należy także uwzględnić, że artykuł 9 dyrektywy (pod tytułem *Przetwarzanie danych osobowych i wolność wypowiedzi)* pozwala państwom członkowskim na 'wprowadzenie możliwości wyłączenia lub odstąpienia od [określonych przepisów dyrektywy] w przypadku przetwarzania danych osobowych wyłącznie w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego jedynie wówczas, gdy jest to konieczne dla pogodzenia prawa do zachowania prywatności z przepisami dotyczącymi wolności wypowiedzi'.

[81] Patrz np. 'Przykład 21: Dane związane z inteligentnym opomiarowaniem (tzw. smart metering) uzyskiwane w celu wykrywania oszustw w wykorzystywaniu energii' na str. 67 w opinii 3/2013 Grupy Roboczej w sprawie ograniczenia celu (cytowanej powyżej w przypisie 9).

„wagi" temu interesowi. Im bardziej istotny jest interes publiczny lub interes szerszej społeczności oraz im bardziej uznane i oczekiwane jest przez wspólnotę oraz osoby, których dane dotyczą, że administrator może podjąć działanie oraz przetwarzać dane w ramach tych interesów, tym większa waga takiego prawnie uzasadnionego interesu na szali.

Z drugiej strony „prywatne egzekwowanie" prawa nie powinno być wykorzystywane do legitymizacji naruszających praktyk, które mogłyby być, jeżeli miałyby być przeprowadzane przez organizacje rządowe, zabronione zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka, na podstawie tego, że te czynności organów publicznych naruszałyby prywatność osób, których dane dotyczą, bez spełnienia rygorystycznego testu na podstawie art. 8 ust. 2 EKPCz.

iii) Inne prawnie uzasadnione interesy

W niektórych przypadkach, jak to już zostało omówione w Części III.2, kontekst, w którym prawnie uzasadniony interes się pojawia, może być bliski jednemu z kontekstów, w których można wykorzystać którąś z innych podstaw prawnych, w szczególności, podstawy prawne zawarte w art. 7 lit. b) (umowa), 7 lit. c) (zobowiązanie prawne), lub 7 lit. e) (zadanie publiczne), mogą znajdować zastosowanie. Na przykład czynność przetwarzania danych może nie być ściśle niezbędna, ale ciągle może być powiązana z wykonaniem umowy – lub prawo może jedynie dopuszczać, ale nie wymagać, aby określone dane były przetwarzane. Jak zobaczyliśmy, nie zawsze może być proste poprowadzenie jasnej linii oddzielającej różne podstawy, jednakże czyni to tym bardziej ważną analizę testu równowagi na podstawie art. 7 lit. f).

Także tutaj, jak również we wszystkich możliwych przypadkach jak dotąd nie wspomnianych, im bardziej istotny jest interes administratora oraz im bardziej jasno uznany, a także im bardziej oczekiwane jest w szerszej społeczności, że administrator może powziąć działania oraz przetwarzać dane dążąc do takiego interes, tym więcej taki interes waży na szali[82]. To doprowadza nas do następnych, bardziej ogólnych punktów.

iv) Prawne oraz kulturowe/społeczne uznanie zasadności interesu

We wszystkich powyższych kontekstach z pewnością znaczące jest, czy prawo UE lub prawo państw członkowskich konkretnie zezwala (nawet jeżeli tego nie wymaga), aby administratorzy podejmowali kroki w celu dążenia do publicznego lub prywatnego interesu o, którym mowa. Istnienie należycie przyjętych, niewiążących wytycznych wydanych przez ciała administracyjne, na przykład przez agencje regulacyjne, zachęcające administratorów do przetwarzania danych w dążeniu do tego interesu także ma znaczenie.

Zgodność z niewiążącymi wytycznymi przyjętymi przez organy ochrony danych lub inne odpowiednie ciała w odniesieniu do sposobów przetwarzania danych także będzie prawdopodobnie pozytywnie przyczyniać się do pozytywnej oceny równowagi. Kulturowe oraz społeczne oczekiwania, nawet jeżeli nie znajdują dokładnego odbicia w legislacyjnych lub regulacyjnych instrumentach, mogą także odgrywać rolę, oraz mogą pomagać zmienić równowagę w obu kierunkach.

[82] Oczywiście ocena musi również obejmować refleksję nad możliwymi szkodami ponoszonymi przez administratora, strony trzecie lub szerszą społeczność, jeżeli przetwarzanie danych nie będzie miało miejsca.

Im bardziej uznane w prawie, w innych instrumentach regulacyjnych – wiążących dla administratora czy też nie – czy nawet w kulturze danej społeczności bez konkretnych podstaw prawnych, że administratorzy mogą podejmować działania oraz przetwarzać dane w dążeniu do danego interesu, tym więcej taki interes waży na szali[83].

b) Wpływ na osoby, których dane dotyczą

Spoglądając na drugą stronę wagi, wpływ przetwarzania na interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, jest kluczowym kryterium. Pierwszy podrozdział poniżej analizuje ogólnie warunki, jak ocenić wpływ na osobę, której dane dotyczą.

Kilka elementów może być tutaj użytecznych i są one przeanalizowane w dalszych podrozdziałach, włączając w to charakter danych osobowych, sposób, w jaki informacja jest przetwarzana, racjonalne oczekiwania osób, których dane dotyczą, oraz status administratora oraz osoby, której dane dotyczą. Omówimy także krótko kwestie związane z potencjalnymi źródłami ryzyka, które mogą prowadzić do wywarcia wpływu na zainteresowane osoby, stopień poważności tego wpływu na zainteresowane osoby oraz prawdopodobieństwo tego, że takie wpływy się urzeczywistnią.

i) Ocena wpływu

Przy ocenie wpływu[84] powinny być wzięte pod uwagę zarówno pozytywne, jak i negatywne konsekwencje. Może to objąć potencjalne przyszłe decyzje lub działania osób trzecich, oraz sytuacje, w których przetwarzanie może prowadzić do wykluczenia lub dyskryminacji osób, zniesławienia lub, bardziej szeroko, sytuacji, w których istnieje ryzyko uszczerbku dla reputacji, pozycji negocjacyjnej lub autonomii osoby, której dane dotyczą.

Obok niekorzystnych rezultatów, które mogą być konkretnie przewidziane, istnieje potrzeba, aby wziąć pod uwagę także szerszy wpływ emocjonalny, taki jak irytacja, strach, stres, które mogą być skutkiem utraty przez osobę, której dane dotyczą kontroli, nad swoimi informacjami osobistymi lub zdania sobie sprawy z tego, że mogą one być wykorzystane niezgodnie z przeznaczeniem lub naruszone, - np. poprzez upublicznienie w Internecie. Należy również należycie uwzględnić hamujący wpływ na chronione zachowania, takie jak wolność prowadzenia badań lub wolność słowa, które mogą być skutkiem ciągłego monitorowania/śledzenia, muszą być należycie uwzględnione.

Grupa Robocza podkreśla, że kluczowe jest, aby zrozumieć, że dany „wpływ" jest znaczenie szerszym pojęciem niż krzywda lub szkoda dla jednej lub większej liczby konkretnych osób, której dane dotyczą. „Wpływ", tak jak to pojęcie jest używane w niniejszej opinii, pokrywa każdą możliwą (potencjalną lub faktyczną) konsekwencję przetwarzania danych. Dla potrzeb jasności podkreślamy również, że pojęcie to nie jest związane z pojęciem naruszenia ochrony

[83] Interes ten nie może być jednak wykorzystany do legitymizacji naruszających praktyk, które nie spełniłyby testu z artykułu 8 ust. 2 EKPCz.

[84] Ocenę wpływu należy rozumieć w kontekście artykułu 7 lit. f). Innymi słowy, nie odnosimy się do 'analizy ryzyka' ani 'oceny wpływu na ochronę danych' w rozumieniu projektu rozporządzenia (artykuły 33 i 34) i różnych zmian do niego proponowanych przez LIBE. Kwestia, jaką metodologię należy stosować przy 'analizie ryzyka' czy też 'ocenie wpływu na ochronę prywatności' wykracza poza zakres niniejszej opinii. Z drugiej strony należy pamiętać, że – w ten czy inny sposób – analiza wpływu zgodnie z artykułem 7 lit. f) może stanowić istotną część każdej 'oceny ryzyka' czy też 'oceny wpływu na ochronę prywatności' i może również pomóc określić sytuacje, w których należy konsultować się z organem ochrony danych.

danych i jest znacznie szersze niż wpływy, które mogą być skutkiem naruszenia ochrony danych. Zamiast tego, pojęcie wpływu, tak jak jest ono tutaj używane, obejmuje różne sposoby, w jakie osoba może być dotknięta – pozytywnie lub negatywnie – przez przetwarzanie jej danych osobowych[85].

Jest także ważne, aby zrozumieć, że zazwyczaj szereg powiązanych i niepowiązanych wydarzeń może łącznie prowadzić do ostatecznie negatywnego wpływu na osobę, której dane dotyczą i może być trudno zidentyfikować, która operacja przetwarzania danych, przeprowadzona przez którego administratora odegrała kluczową rolę w negatywnym wpływie.

Biorąc pod uwagę, że rozpoczęcie postępowania odszkodowawczego za poniesioną krzywdę lub szkodę jest często trudne dla osób, których dane dotyczą w tym kontekście, nawet jeżeli sam skutek jest bardzo rzeczywisty, tym bardziej ważne jest, aby skupić się na zapobieganiu oraz zapewnianiu, że operacje przetwarzania danych mogą być przeprowadzone tylko wtedy, gdy nie niosą one za sobą ryzyk lub niosą bardzo małe ryzyko nadmiernego negatywnego wpływu na interesy lub podstawowe prawa i wolności osób, których dane dotyczą.

Przy ocenie wpływ, terminologia oraz metodologia tradycyjnych ocen ryzyka może być użyteczna do pewnego stopnia, i z tego względu niektóre elementy tej metodologii zostaną pokrótce omówione poniżej. Jednakże całościowa metodologia oceny wpływu – w kontekście art. 7 lit. f) lub szerzej – wykraczałaby poza zakres niniejszej opinii.

W tym kontekście, jak i gdzie indziej, istotne jest zidentyfikowanie źródeł potencjalnych wpływów na osoby, których dane dotyczą.

Prawdopodobieństwo, że ryzyko może się urzeczywistnić, jest jednym z elementów, które należy wziąć pod uwagę. Na przykład dostęp do Internetu, wymiana danych ze stronami spoza UE, połączenia z innymi systemami oraz wysoki stopień heterogeniczności lub zmienności systemów może stanowić czułe punkty, które hakerzy mogą wykorzystać. Ryzykowne źródła niosą za sobą względnie wysokie prawdopodobieństwo, że ryzyko naruszenia ochrony danych się urzeczywistni. Odwrotnie, homogeniczny, stabilny system, który nie ma połączeń i jest odłączony od Internetu, niesie dużo mniejsze prawdopodobieństwo naruszenia ochrony danych.

Innym elementem oceny ryzyka jest stopień poważności konsekwencji urzeczywistnionego ryzyka. Stopień poważności może wahać się od niskich poziomów (takich jak irytująca konieczność ponownego podania danych kontaktowych utraconych przez administratora danych) do bardzo wysokich poziomów (jak utrata życia, gdy informacje o lokalizacji chronionych osób dostaną się w ręce przestępców lub gdy zasilanie jest zdalnie odcięte

[85] Ryzyko szkody finansowej, np. jeżeli naruszenie ochrony danych prowadzi do ujawnienia informacji finansowych, które miały znajdować się w bezpiecznym środowisku i to ostatecznie prowadzi do kradzieży tożsamości lub innych form oszustwa, bądź też ryzyko obrażenia ciała, bólu, cierpienia i pogorszenia się jakości życia, co mogłoby ostatecznie wynikać np. z nieuprawnionej zmiany historii choroby, oraz następujące niewłaściwe leczenie pacjenta, zawsze należy brać odpowiednio pod uwagę, choć w żadnym razie nie jest to ograniczone do sytuacji objętych zakresem artykułu 7 lit. f). Jednocześnie takie zagrożenia to nie jedyne zagrożenia, które należy uwzględnić przy ocenie wpływu zgodnie z artykułem 7 lit. f).

poprzez inteligentne urządzenia pomiarowe w przypadku krytycznej pogody lub osobistego stanu zdrowia).

Te dwa kluczowe elementy – prawdopodobieństwo tego, że ryzyko się urzeczywistni z jednej strony, oraz stopień poważności konsekwencji z drugiej – oba przyczyniają się do ogólnej oceny potencjalnego wpływu.

Na koniec przy stosowaniu metodologii należy pamiętać, że ocenianie wpływu na podstawie art. 7 lit. f) nie może prowadzić do mechanicznych oraz czysto ilościowych działań. W tradycyjnych scenariuszach oceny ryzyka, „stopień poważności" może także brać pod uwagę liczbę osób, na które wpływ może zostać potencjalnie wywarty. Jednakże należy pamiętać, że przetwarzanie danych osobowych mających wpływ na mniejszość osób, których dane dotyczą – lub nawet jedynie na pojedyncze jednostki – ciągle wymaga bardzo starannej analizy, w szczególności jeżeli taki wpływ na każdą potencjalną jednostkę jest potencjalnie znaczący.

ii) Charakter danych

Na początku ważne jest, aby ocenić, czy przetwarzanie dotyczy danych szczególnie chronionych, czy to dlatego, że należą do szczególnych kategorii danych zgodnie z art. 8 dyrektywy, lub z innych powodów, jak np. w przypadku danych biometrycznych, informacji genetycznych, danych komunikacyjnych, danych lokalizacyjnych oraz innych typów informacji osobowych wymagających szczególnej ochrony[86].

Tytułem przykładu w opinii Grupy Roboczej, co do zasady, wykorzystanie biometrii do ogólnych wymogów bezpieczeństwa własności lub osób jest uznawane za prawnie uzasadniony interes, wobec którego nadrzędne są interesy oraz podstawowe prawa i wolności osoby, której dane dotyczą. Z drugiej strony dane biometryczne, takie jak odciski palców lub skan tęczówki oka, mogą być wykorzystane dla bezpieczeństwa obszarów o wysokim ryzyku, takich jak laboratoria przeprowadzające badania na groźnych wirusach, przy założeniu, że administrator przedstawił konkretne dowody występowania znaczącego ryzyka[87].

Generalnie, im bardzie wrażliwe są informacje, tym więcej konsekwencji może z tego wyniknąć dla osoby, której dane dotyczą. Jednakże nie oznacza to, że dane, które same w sobie mogą wydać się nieszkodliwe, mogą być dowolnie przetwarzane na podstawie art. 7 lit. f). Istotnie, nawet takie dane, w zależności od sposobu, w jaki są przetwarzane, mogą mieć znaczący wpływ na osoby, jak to zostanie pokazane w podrozdziale (iii) poniżej.

W tym względzie fakt, czy dane zostały upublicznione prze osobę, której dane dotyczą czy przez osobę trzecią, może mieć znaczenie. Istotne jest tutaj przede wszystkim to, aby podkreślić, że dane osobowe, nawet jeżeli zostały upublicznione, ciągle są uważane za dane

[86] Dane biometryczne i informacje genetyczne uznawane są za szczególne kategorie danych we wniosku Komisji dotyczącym rozporządzenia o ochronie danych, odczytywanym łącznie ze zmianami proponowanymi przez Komisję LIBE. Patrz poprawka 103 do artykułu 9 w Ostatecznym sprawozdaniu Komisji LIBE. W kwestii związku artykułów 7 i 8 z dyrektywą 95/46/WE patrz Część II.1.2 powyżej na str. 14-15.

[87] Patrz opinia 3/2012 Grupy Roboczej Artykułu 29 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP 193). Tytułem innego przykładu, w swojej opinii 4/2009 dotyczącej Światowej Agencji Antydopingowej (cytowanej powyżej w przypisie 32) Grupa Robocza podkreśliła, że artykuł 7 lit. f) nie byłby ważną podstawą przetwarzania danych medycznych i danych dotyczących wykroczeń w kontekście dochodzeń antydopingowych, ze względu na 'wagę naruszeń prywatności'. Przetwarzanie danych powinno być przewidziane prawem i spełniać wymogi artykułu 8 ust. 4 i 5 dyrektywy.

osobowe, i z tego względu ich przetwarzanie nadal wymaga odpowiednich zabezpieczeń[88]. Nie ma blankietowego pozwolenia na ponowne wykorzystanie oraz dalsze przetwarzanie publicznie dostępnych danych osobowych na podstawie art. 7 lit. f).

Biorąc to pod uwagę okoliczność, że dane osobowe są publicznie dostępne, może być uznany za czynnik w ocenie, w szczególności jeżeli publikacja została przeprowadzona w rozsądnym oczekiwaniu dalszego wykorzystania danych dla pewnych celów (na przykład dla celów badań lub dla celów związanych z przejrzystością oraz rozliczalnością).

iii) Sposób, w jaki dane są przetwarzane

Ocena wpływu w szerszym znaczeniu może obejmować rozważenie tego, czy dane są publicznie ujawnione lub w inny sposób udostępnione dużej liczbie osób, lub czy duża ilość danych osobowych jest przetwarzana lub zestawiana z innymi danymi (na przykład w przypadku profilowania, dla celów handlowych lub wdrażania prawa czy też innych celów). Potencjalnie nieszkodliwe dane, kiedy są przetwarzane na dużą skalę oraz zestawiane z innymi danymi mogą prowadzić do konkluzji na temat bardziej wrażliwych danych, jak wykazano to w scenariuszu 3, ilustrującym związek między wzorami konsumpcji pizzy oraz składkami ubezpieczenia zdrowotnego.

Obok potencjalnego prowadzenia do przetwarzania bardziej wrażliwych danych, takie analizy mogą także prowadzić do dziwnych, niespodziewanych, a czasami także niedokładnych przewidywań, na przykład dotyczących zachowania lub osobowości danych jednostek. W zależności od charakteru lub wpływu tych przewidywań, może to w poważnym stopniu naruszać prywatność osób[89].

Grupa Robocza zwróciła uwagę także w poprzedniej opinii na ryzyka będące częścią określonych rozwiązań dotyczących bezpieczeństwa (włączając w to zapory ogniowe, antywirusowe lub antyspamowe), jako że mogą prowadzić do zastosowania głębokiej inspekcji pakietów na dużą skalę, co może mieć znaczący wpływ na ocenę równowagi praw[90].

Ogólnie, im bardziej negatywny lub niepewny może być wpływ na przetwarzanie, tym mniej prawdopodobne jest to, że przetwarzanie będzie uznane, po wyważeniu, za prawnie uzasadnione. Dostępność alternatywnych metod osiągnięcia celów administratora, z mniej negatywnym wpływem na osobę, której dane dotyczą, byłaby z pewnością zasadną refleksją w tym kontekście. Gdy to właściwe, ocena wpływu na ochronę danych oraz prywatność może być wykorzystana do oceny tego, czy stanowi to możliwość.

iv) Racjonalne oczekiwania osoby, której dane dotyczą

Racjonalne oczekiwania osoby, której dane dotyczą, w odniesieniu do wykorzystania oraz ujawnienia danych są również bardzo istotne w tym przypadku. Jak również podkreślono w

[88] Patrz opinia Grupy Roboczej 3/2013 w sprawie ograniczenia celu (cytowana w przypisie 9 powyżej) oraz opinia Grupy Roboczej 6/2013 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (ISP), przyjęta 5 czerwca 2013 r. (WP 207).

[89] Patrz Część III.2.5 oraz Załącznik 2 (Big data i otwarte dane) opinii w sprawie ograniczenia celu (cytowanej powyżej w przypisie 9).

[90] Patrz Część 3.1 opinii Grupy Roboczej 1/2009 w sprawie wniosków zmieniających dyrektywę 2002/58/WE o prywatności i łączności elektronicznej (dyrektywę o prywatności i łączności elektronicznej) (WP 159).

odniesieniu do analizy zasady ograniczenia celu[91], jest „ważne, aby rozważyć, czy status administratora danych[92], charakter związku lub dostarczone usługi[93], bądź właściwe zobowiązania prawne lub umowne (lub inne obietnice poczynione w momencie zbierania danych) mogą dać początek racjonalnym oczekiwaniom ściślejszej poufności oraz ściślejszego ograniczenia dalszego wykorzystania. Generalnie im bardziej szczegółowy oraz restrykcyjny kontekst zbierania, tym bardziej prawdopodobne, że będzie więcej ograniczeń wykorzystania. Ponownie konieczne jest, aby wziąć pod uwagę raczej rzeczywisty kontekst niż po prostu opierać się na tekście napisanym drobnym drukiem.

v) Status administratora danych oraz osoby, której dane dotyczą

Status osoby, której dane dotyczą, oraz administratora danych jest również istotny przy ocenie wpływu przetwarzania. W zależności od tego, czy administrator jest osobą czy małą organizacją, dużą wielonarodową firmą czy podmiotem sektora publicznego, oraz od konkretnych okoliczności, jego pozycja może być bardziej lub mniej dominująca w odniesieniu do osoby, której dane dotyczą. Duża wielonarodowa firma może, na przykład, mieć więcej zasobów i być w lepszej pozycji negocjacyjnej niż pojedyncza osoba, której dane dotyczą, i z tego względu może być w lepszej pozycji do nałożenia na osobę, której dane dotyczą tego, co uznaje za swój „prawnie uzasadniony interes". Może być to jeszcze bardziej prawdziwe, jeżeli firma posiada pozycję dominującą na rynku. Jeżeli pozostanie to niesprawdzone, może dziać się to ze szkodą dla pojedynczych osób, których dane dotyczą. Tak, jak ochrona konsumentów oraz prawa konkurencji pomagają zapewnić, że ta siła nie zostanie wykorzystana w niewłaściwy sposób, prawo ochrony danych może również odgrywać znaczącą rolę w zapewnianiu, że prawa oraz interesy osób, których dane dotyczą, nie będą nadmiernie naruszane.

Z drugiej strony, status osoby, której dane dotyczą, jest również istotny. Podczas gdy co do zasady test równowagi powinien odnosić się do statystycznej jednostki, konkretne sytuacje powinny prowadzić do podejścia opartego na poszczególnych przypadkach: na przykład, właściwe byłoby rozważenie czy osoba, której dane dotyczą jest dzieckiem[94] lub czy w inny sposób należy do bardzie narażonej części populacji, wymagającej szczególnej ochrony, jak np. chorzy umysłowo, ubiegający się o azyl czy osoby starsze. Pytanie, czy osoba, której dane dotyczą, jest pracownikiem, studentem, pacjentem czy w jakiś inny sposób istnieje nierównowaga pomiędzy pozycją osoby, której dane dotyczą, a administratorem, musi także z pewnością być istotne. Ważne jest, aby ocenić efekt przetwarzania dla poszczególnych osób.

Na koniec ważne jest, aby podkreślić, że nie wszystkie negatywne wpływy na osoby, których dane dotyczą, mają taką samą wagę. Celem przewidzianych w art. 7 lit. f) działań dotyczących równoważenia nie jest zapobieżenie jakiemukolwiek negatywnemu wpływowi na osobę, której dane dotyczą. Jego celem jest raczej zapobieżenie nieproporcjonalnemu wpływowi. Jest to kluczowa różnica. Na przykład publikacja dobrze udokumentowanych oraz

[91] Patrz strony 24-25 opinii 3/2013 w sprawie ograniczenia celu (cytowanej powyżej w przypisie 9).

[92] 'Np. adwokat lub lekarz'.

[93] 'Np. usługi przetwarzania w chmurze do zarządzania dokumentami osobowymi, usługi e-mailowe, kalendarze, e-czytniki wyposażone w funkcję robienia notatek oraz różne aplikacje do tzw. life-loggingu (czyli zapisywania materiału z całego dnia naszego życia)

[94] Patrz opinia Grupy Roboczej 2/2009 w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół), przyjęta 11.02.2009 r. (WP 160). Niniejsza opinia kładzie nacisk na szczególną wrażliwość dziecka, a w przypadku, gdy dziecko jest reprezentowane, na potrzebę wzięcia pod uwagę najlepszego interesu dziecka a nie interesu jego przedstawiciela.

dokładnych artykułów prasowych na temat rzekomej korupcji rządu może spowodować szkody dla zaangażowanych urzędników rządowych oraz może prowadzić do znaczących konsekwencji, włączając w to utratę reputacji, utratę wyborców, lub uwięzienie, jednak ciągle znajduje podstawę w art. 7 lit. f)[95].

c) Tymczasowa równowaga

Przy wyważaniu interesów oraz praw, jak to opisano powyżej, środki podjęte przez administratora w celu zapewnienia zgodności z jego ogólnymi obowiązkami wynikającymi z dyrektywy, obejmującymi proporcjonalność oraz przejrzystość, w wielkim stopniu przyczynią się do zapewnienia, że administrator danych spełnia wymogi art. 7 lit. f). Pełna zgodność powinna oznaczać, że wpływ na osoby jest ograniczony, że istnieje *mniejsze prawdopodobieństwo*, że interesy lub prawa i wolności osób, których dane dotyczą zostaną naruszone i z tego względu jest *bardziej prawdopodobne*, że administrator danych może oprzeć się na art. 7 lit. f). Powinno to zachęcić to administratorów do większej zgodności ze wszystkim horyzontalnymi przepisami dyrektywy[96].

Nie oznacza to jednak, że zgodność z tymi horyzontalnymi wymogami zawsze jako taka będzie wystarczająca do zapewnienia podstawy prawnej w postaci art. 7 lit. f) dyrektywy. Istotnie, w takiej sytuacji art. 7 lit. f) byłby zbędny lub stałby się luką w prawie, która uczyniłaby cały art. 7 zbędnym, co wymaga odpowiedniej, konkretnej podstawy prawnej dla przetwarzania.

Z tego powodu ważne jest, aby przeprowadzić dalszą ocenę w ramach wyważenia w sytuacjach, gdy – opierając się na wstępnej analizie – nie jest jasne, w którą stronę równowaga powinna być zapewniona. Administrator powinien rozważyć, czy możliwe jest wprowadzenie dodatkowych środków, wykraczających poza zgodność z horyzontalnymi postanowieniami dyrektywy, aby pomóc zredukować nadmierny wpływ przetwarzania na osoby, których dane dotyczą.

Dodatkowe środki mogą obejmować na przykład zapewnianie łatwo wykonalnego oraz dostępnego mechanizmu w celu zapewnienia osobie, której dane dotyczą, bezwarunkowej możliwości wykorzystania mechanizmu opt-out w odniesieniu do przetwarzania. Te dodatkowe mechanizmy mogą w niektórych (ale nie we wszystkich) przypadkach pomóc przechylić równowagę oraz pomóc zapewnić, że przetwarzanie może być oparte na art. 7 lit. f), jednocześnie chroniąc prawa oraz interesy osób, których dane dotyczą.

d) Dodatkowe zabezpieczenia (środki ochronne) stosowane przez administratora

Jak to wyjaśniono powyżej, sposób, w jaki administrator zastosowałby odpowiednie środki może w niektórych sytuacjach „przechylić równowagę" na skali. To, czy wynik jest akceptowalny, będzie zależeć od oceny całości. Im bardziej znaczący wpływ na osobę, której dane dotyczą, tym większa uwaga powinna być poświęcona odpowiednim zabezpieczeniom.

[95] Jak wyjaśniono powyżej, należy również wziąć pod uwagę wszelkie istotne wyłączenia dla przetwarzania do celów dziennikarskich zgodnie z artykułem 9 dyrektywy.

[96] W kwestii ważnej roli 'zgodności horyzontalnej' patrz także str. 54 opinii Grupy Roboczej 3/2013 w sprawie ograniczenia celu, cytowanej w przypisie 9 powyżej.

Przykłady odpowiednich środków mogą obejmować, m.in., restrykcyjne ograniczenie ilości zbieranych danych lub natychmiastowe usunięcie danych po ich wykorzystaniu. Choć niektóre z tych środków mogą być już obowiązkowe na mocy dyrektywy, są często skalowalne oraz pozostawiają miejsce administratorom do zapewnienia lepszej ochrony osób, których dane dotyczą. Na przykład administrator może zbierać mniej danych lub zapewnić dodatkowe informacje w porównaniu do tego, co jest konkretnie wymienione w art. 10 oraz 11 dyrektywy.

W niektórych innych przypadkach środki ochronne nie są *wyraźnie* wymagane w dyrektywie, ale mogą być w przyszłości wymagane na podstawie proponowanego rozporządzenia lub są one wymagane tylko w konkretnych sytuacjach, takich jak:

- środki organizacyjne i techniczne w celu zapewnienia, że dane nie mogą być wykorzystane do podjęcia decyzji lub innych działań w odniesieniu do osób („oddzielenie funkcjonalne", częste w kontekście badań)
- rozległe zastosowanie technik anonimizacyjnych
- agregowanie danych
- technologie wzmacniające prywatność, prywatność w fazie projektowania, ocena wpływu na prywatność i ochronę danych
- zwiększona przejrzystość
- ogólne oraz bezwarunkowe prawo do mechanizmu opt-out
- możliwość przenoszenia danych oraz powiązane środki uprawniające osobę, której dane dotyczą

Grupa Robocza zauważa, że w odniesieniu do niektórych kluczowych kwestii, obejmujących oddzielenie funkcjonalne oraz techniki anonimizacyjne, pewne wytyczne zostały już przedstawione w odpowiednich częściach jej opinii w sprawie ograniczenia celu, w sprawie otwartych danych data oraz w sprawie technik anonimizacyjnych[97].

Jeżeli chodzi o techniki pseudonimizacyjne oraz szyfrowanie, Grupa Robocza chciałaby podkreślić, że jeżeli dane nie umożliwiają bezpośredniej identyfikacji, nie wpływa to jako takie na uznanie legalności przetwarzania: nie powinno być to rozumiane jako zmiana nielegalnego przetwarzania w legalne[98].

Jednocześnie pseudonimizacja i szyfrowanie, podobnie jak wszystkie inne techniczne i organizacyjne środki wprowadzone w celu ochrony informacji osobowych, będą odgrywały rolę w odniesieniu do oceny potencjalnego wpływu przetwarzania na osobę, której dane dotyczą, i w ten sposób mogą w niektórych przypadkach odegrać rolę w przechyleniu

[97] Patrz Części III.2.3, III.2.5 oraz Załącznik 2 opinii Grupy Roboczej 3/2013 w sprawie ograniczenia celu, cytowanej w przypisie 9 powyżej, w kwestii dalszego przetwarzania do celów historycznych, statycznych i naukowych oraz big data i otwartych danych; patrz również właściwe części opinii Grupy Roboczej 6/2013 w sprawie otwartych danych (cytowanej w przypisie 88 powyżej) oraz opinii 5/2014 w sprawie technik anonimizacji.

[98] W tej kwestii patrz: poprawki przegłosowane przez Komisję LIBE w Ostatecznym sprawozdaniu Komisji LIBE, a w szczególności poprawka 15 w motywie 38 łącząca pseudonimizację i prawnie uzasadnione oczekiwania osoby, której dane dotyczą.

równowagi na korzyść administratora. Wykorzystanie mniej ryzykownych form przetwarzania danych osobowych (na przykład danych osobowych, które są szyfrowane podczas przechowywania czy transmisji lub danych osobowych, które są mniej bezpośrednio i w mniej łatwy sposób identyfikowalne), powinno generalnie oznaczać, że prawdopodobieństwo naruszenia interesów lub podstawowych praw i wolności osób, których dane dotyczą, jest zmniejszone.

W połączeniu z tymi środkami ochronnymi – oraz ogólną oceną równowagi – Grupa Robocza chciałaby podkreślić trzy konkretne kwestie, które często odgrywają kluczową rolę w kontekście art. 7 lit. f):

- związek pomiędzy testem równowagi, przejrzystością oraz zasadą rozliczalności;
- prawo osoby, której dane dotyczą, do wyrażenia sprzeciwu wobec przetwarzania ora, poza sprzeciwem, dostępność mechanizmu opt-out bez żadnej potrzeby uzasadnienia, oraz
- uprawnienie osób, których dane dotyczą: możliwość przenoszenia danych oraz dostępność wykonalnego mechanizmu dla osób, których dane dotyczą, pozwalającego na dostęp, zmianę, usunięcie, przekazanie lub dalsze przetwarzanie (lub pozwolenie osobom trzecim na dalsze przetwarzanie) ich własnych danych.

Z uwagi na stopień ich ważności, tematy te zostaną przedyskutowane w oddzielnych częściach.

III. 3.5. Rozliczalność oraz przejrzystość

Najpierw, zanim rozpocznie się operacja przetwarzania na podstawie art. 7 lit. f), administrator jest odpowiedzialny za ocenę, czy ma prawnie uzasadniony interes, czy przetwarzanie jest niezbędne dla tego prawnie uzasadnionego interesu oraz wobec interesu nadrzędne są interesy oraz prawa osób, których dane dotyczą, w konkretnej sprawie.

W tym sensie art. 7 lit. f) jest oparty na zasadzie rozliczalności. Administrator musi przeprowadzić uważany oraz skuteczny test zawczasu, opierając się raczej na konkretnych okolicznościach sprawy niż na abstrakcyjnych założeniach, biorąc pod uwagę racjonalne oczekiwania osób, których dane dotyczą. Jako kwestię dobrej praktyki, gdzie to odpowiednie, przeprowadzenie testu powinno być udokumentowane w wystarczająco szczegółowy oraz przejrzysty sposób, tak aby uzupełnione oraz poprawne zastosowanie testu mogło być zweryfikowane – kiedy to konieczne – przez odpowiednie zainteresowane osoby, włączając w to osoby, których dane dotyczą, oraz organy ochrony danych, oraz ostatecznie sądy.

Administrator w pierwszej kolejności definiuje prawnie uzasadniony interes oraz przeprowadza test równowagi, jednak niekoniecznie jest to ostateczna definitywna ocena: jeżeli, w rzeczywistości, interes, do którego dąży, nie jest tym, który określił administrator lub jeżeli administrator zdefiniował interes w niewystarczająco szczegółowy sposób, równowaga musi być ponownie oceniona, opierając się na tym, aby rzeczywisty interes został określony albo przez organ ochrony danych albo sąd[99]. Tak jak i w innych kluczowych aspektach

[99] Np. w związku ze skargą lub sprzeciwem z artykułu 14.,

ochrony danych, takich jak identyfikacja administratora danych czy określenie celu[100], to co liczy się w rzeczywistości wykracza poza zapewnienia administratora.

Pojęcie rozliczalności jest ściśle powiązane z przejrzystością. W celu umożliwienia osobom, których dane dotyczą, wykonania swoich praw oraz, w szerszym rozumieniu, pozwolenia na nadzór publiczny przez zainteresowane osoby, Grupa Robocza zaleca, żeby administratorzy wyjaśnili osobom, których dane dotyczą, w prosty oraz przyjazny użytkownikowi sposób powody, dla których wierzą oni, że wobec ich interesów nie są nadrzędne interesy oraz podstawowe prawa i wolności osób, których dane dotyczą, oraz także wyjaśnili im podjęte w celu ochrony danych zabezpieczenia, włączając, gdzie to odpowiednie, prawo do zastosowania mechanizmu opt-out wobec przetwarzania[101].

W tym aspekcie Grupa Robocza podkreśla, że prawo ochrony konsumentów, w szczególności prawo chroniące konsumentów przed nieuczciwymi praktykami handlowymi, jest również tutaj bardzo istotne.

Jeżeli administrator ukrywa ważne informacje dotyczące przewidywanego dalszego wykorzystania danych, w ujęciu prawniczym, napisanych drobnym drukiem w umowie, to może to naruszyć zasady ochrony konsumentów dotyczące nieuczciwych przepisów umownych (w tym zakaz „zaskakujących warunków"), oraz nie wypełni to wymogów art. 7 lit. a), mówiącego o ważnej świadomej zgodzie, lub wymogów art. 7 lit. f) w odniesieniu do racjonalnych oczekiwań osoby, której dane dotyczą oraz ogólnie akceptowalnej równowagi interesów. Oczywiście wzbudza to także wątpliwości dotyczące zgodności z art. 6, jeśli chodzi o potrzebę uczciwego i zgodnego z prawem przetwarzania danych osobowych.

Na przykład w wielu przypadkach użytkownicy „darmowych" usług internetowych, takich jak wyszukiwanie, poczta elektroniczna, media społecznościowe, przechowywanie danych oraz inne aplikacje internetowe oraz mobilne, nie są do końca świadomi zakresu, w jakim informacje na temat ich działania są przechowywane oraz analizowane w celu wygenerowania wartości dla dostarczycieli usług i z tego względu nie przejmują się obecnym ryzykiem.

W celu zapewnienia uprawnień dla osób, których dane dotyczą, w tych sytuacjach, pierwszym koniecznym – ale w żadnym razie niewystarczającym samodzielnie – warunkiem wstępnym[102] jest wyjaśnienie, że usługi nie są darmowe, a raczej, że użytkownicy płacą za ich wykorzystanie własnymi danymi osobowymi. Warunki oraz środkach ochronne, z zastrzeżeniem których dane mogą być wykorzystywane, muszą być jasno przedstawione w

[100] Patrz opinie cytowane w przypisie 9.

[101] Jak wyjaśniono na str. 46 opinii Grupy Roboczej 3/2013 w sprawie ograniczenia celu (cytowanej w przypisie 9 powyżej), w przypadku profilowania oraz decyzji zautomatyzowanych, 'w celu zapewnienia przejrzystości, osobom, których dane dotyczą/konsumentom należy zapewnić dostęp to ich 'profili', jak również do informacji na temat logiki podejmowania decyzji (algorytmu), która doprowadziła do stworzenia profilu. Innymi słowy: organizacje powinny ujawnić informacje na temat ich kryteriów decyzyjnych. Jest to kluczowe zabezpieczenie i tym bardziej ważne w świecie big data'. Niezwykle istotnym czynnikiem, który również należy uwzględnić w przypadku wyważania, jest fakt, czy organizacja oferuje taką przejrzystość czy też nie.

[102] W kwestii dalszych możliwych środków ochronnych w odniesieniu do coraz powszechniejszych sytuacji, w których konsumenci płacą swoimi danymi osobowymi, patrz Część III.3.6, w szczególności str. 47-48 'Przyjazne dla prywatności rozwiązania alternatywne w stosunku do „bezpłatnych" usług internetowych; oraz 'Możliwość przenoszenia danych, 'midata' oraz powiązane kwestie'.

każdym przypadku, tak aby zapewnić ważność zgody z art. 7 lit. a) lub korzystną równowagę zgodnie z art. 7 lit. f)

III.3.6 Prawo do wyrażenia sprzeciwu oraz prawa wykraczające poza nie

a) Prawo do sprzeciwu na podstawie art. 14 dyrektywy

Art. 7 lit. e) oraz f) są szczególne w tym sensie, że chociaż opierają się głównie na obiektywnej ocenie zaangażowanych interesów i praw, pozwalają także na samostanowienie osoby, której dane dotyczą, czy skorzystać z prawa do sprzeciwu[103]: przynajmniej w odniesieniu do tych dwóch podstaw, art. 14 lit. a) dyrektywy stanowi, że („z zastrzeżeniem odmiennych postanowień ustawodawstwa krajowego") osoba, której dane dotyczą, „może wyrazić w dowolnym czasie z ważnych i uzasadnionych przyczyn wynikających z jego konkretnej sytuacji, sprzeciw co do przetwarzania dotyczących jej danych". Dodano także, że w przypadku, gdy sprzeciw jest uzasadniony, nie można już przetwarzać tych danych.

Co do zasady, zgodnie z obecnym prawem, osoba, której dane dotyczą, będzie więc musiała wykazać „ważne, uzasadnione interesy", aby wstrzymać przetwarzanie jej danych osobowych (art. 14 lit. a)), z wyjątkiem kontekstu działań marketingu bezpośredniego, gdzie sprzeciw nie musi być uzasadniony (art. 14 lit. b)).

Nie powinno to być postrzegane jako zaprzeczające testowi równowagi na podstawie art. 7 lit. f), który jest dokonywany 'a priori'": dopełnia on raczej równowagi, w takim sensie, że gdy przetwarzanie jest dozwolone w wyniku rozsądnej oraz obiektywnej oceny różnych praw oraz interesów, które należy wziąć pod uwagę, osoba, której dane dotyczą, posiada *dodatkową* możliwość zgłoszenia sprzeciwu na podstawie jej konkretnej sytuacji. Musiałoby to następnie prowadzić do nowej oceny, biorąc pod uwagę konkretne argumenty przedstawione przez osobę, której dane dotyczą. Ta nowa ocena jest co do zasady ponownie poddawana weryfikacji przez organ ochrony danych lub sądy.

b) Poza prawem do sprzeciwu: rola mechanizmu opt-out jako dodatkowy środek ochronny

Grupa Robocza podkreśla, że nawet jeżeli prawo do wyrażenia sprzeciwu zgodnie z art. 14 lit. a) podlega uzasadnieniu przez osobę, której dane dotyczą, nic nie zapobiega temu, aby administrator zaoferował mechanizm opt-out, który byłby szerszy, i który nie wymagałby dodatkowego wykazania prawnie uzasadnionego interesu (ważnego czy innego), od osoby, której dane dotyczą. Takie bezwarunkowe prawo nie musiałoby być oparte na konkretnej sytuacji osób, których dane dotyczą.

W rzeczywistości, a w szczególności w sytuacjach granicznych, gdzie równowaga jest trudna do osiągnięcia, dobrze zaprojektowany, działający mechanizm opt-out, chociaż niekoniecznie zapewniający osobom, których dane dotyczą, wszystkie elementy, które spełniałyby wymogi

[103] To prawo do wyrażenia sprzeciwu nie powinno być mylone ze zgodą w oparciu o artykuł 7 lit. a), gdzie administrator danych nie może przetwarzać danych przed uzyskaniem takiej zgody. W kontekście artykułu 7 lit. f) administrator może przetwarzać dane, z zastrzeżeniem warunków i zabezpieczeń, o ile osoba, której dane dotyczą, nie wyraziła sprzeciwu. W tym rozumieniu prawo do sprzeciwu można raczej uznać jako specjalną formę opt-out. Więcej szczegółów w opinii Grupy Roboczej 15/2011 w sprawie definicji zgody (cytowanej w przypisie 2).

ważnej zgody zgodnie z art. 7 a), mógłby odegrać ważną rolę w zabezpieczeniu praw oraz interesów osób, których dane dotyczą.

Z tego względu potrzebne jest zniuansowane podejście, które odróżnia sytuację, gdzie zgoda opt-in na mocy art. 7 lit. a) jest wymagana, oraz sytuacje, gdzie wykonalna możliwość zastosowania mechanizmu opt-out wobec przetwarzania (zestawiona z możliwymi innymi dodatkowymi środkami) może przyczynić się do ochrony osób, których dane dotyczą, zgodnie z art. 7 lit. f).

Im szerzej stosowany mechanizm oraz im łatwiejszy do zastosowania opt-out, tym bardziej przyczyni się do przechylenia równowagi na korzyść przetwarzania znajdującego podstawę w art. 7 lit. f).

Przykład: ewolucja podejścia do marketingu bezpośredniego

W celu zobrazowania, jak rozróżnić sprawy, gdzie zgoda na podstawie art. 7 lit. a) jest wymagana, oraz sprawy, gdzie mógłby być zastosowany mechanizm opt-out jako środek ochronny zgodnie z art. 7 lit. f), pomocne jest posłużenie się przykładem marketingu bezpośredniego, dla którego tradycyjnie przewidziano konkretne przepisy dotyczące mechanizmu opt-out, włączone do art. 14 lit. b) dyrektywy. Aby sprostać nowym wyzwaniom technologiczny,, przepis został później uzupełniony, przez konkretne przepisy dyrektywy o prywatności i łączności elektronicznej[104].

Zgodnie z art. 13 dyrektywy o prywatności i łączności elektronicznej dla niektórych typów – bardziej inwazyjnych – działań w zakresie marketingu bezpośredniego (takich jak wiadomości przesyłane na pocztę e-mail oraz automatyczne systemy dzwoniące), zasadą jest zgoda. W ramach wyjątku, przy istniejących relacjach z klientem, w ramach których administrator przesyła reklamy własnych podobnych produktów lub usług, wystarczające jest zapewnienie (bezwarunkowej) możliwości do zastosowania mechanizmu opt-out bez uzasadnienia.

Technologie ewoluowały, co wymagało względnie prostych rozwiązań podążających za podobną logiką dla nowych działań marketingowych.

Po pierwsze, ewoluował sposób, w jaki materiały marketingowe są dostarczane: zamiast prostych wiadomości elektronicznych przesyłanych na skrzynkę, obecnie ukierunkowane reklamy behawioralne wyskakują na smartfonach oraz na ekranach komputera. W najbliższej przyszłości reklamy mogą być także wbudowane w inteligentne przedmioty połączone z Internetem Przedmiotów.

Po drugie, reklamy stają się coraz bardziej konkretnie ukierunkowane: zamiast opierać się na prostych profilach klientów, działania klientów są coraz bardziej śledzone oraz przechowywane zarówno online, jak i offline, oraz analizowane przy użyciu bardziej skomplikowanych automatycznych metod[105].

[104] W kwestii artykułu 13 dyrektywy o prywatności i łączności elektronicznej patrz także Część III.2.4 opinii Grupy Roboczej 3/2013 w sprawie ograniczenia celu (cytowana w przypisie 9 powyżej).

[105] Patrz Część III.2.5 oraz Załącznik 2 (w sprawie big data i otwartych danych) opinii Grupy Roboczej 3/2013 w sprawie ograniczenia celu (cytowanej w przypisie 9 powyżej).

W wyniku tego rozwoju zmienił się przedmiot szukania równowagi: kwestią nie jest już prawo do wolności słowa w handlu, ale przede wszystkim interes ekonomiczny organizacji biznesowych w zakresie poznania ich klientów poprzez śledzenie i monitorowanie ich działań online i offline, co powinno być zrównoważone względem (podstawowych) praw do prywatności i ochrony danych osobowych tych osób oraz ich interesu, aby nie być nadmiernie monitorowanymi.

Ta zmiana w dominujących modelach biznesowych oraz wzrost wartości danych osobowych jako zasobów organizacji biznesowych wyjaśnia ostatnie wymogi uzyskania zgody w tym kontekście zgodnie z art. 5 ust. 3) oraz art. 13 dyrektywy o prywatności i łączności elektronicznej.

Istnieją więc różne konkretne reguły zależące od formy marketingu, obejmujące:
- bezwarunkowe prawo do wyrażenia sprzeciwu wobec marketingu bezpośredniego (zaprojektowane dla kontekstu tradycyjnych wiadomości pocztowych, oraz dla marketingu podobnych produktów) zgodnie z art. 14 lit. b) dyrektywy; art. 7 lit. f) mógłby być podstawą prawną w tym przypadku.;
- wymóg zgody zgodnie artykułem 13 dyrektywy o prywatności i łączności elektronicznej dla automatycznych systemów wywołujących, faksu, wiadomości tekstowych oraz marketingu e-mailingowego (z zastrzeżeniem wyłączeń)[106], oraz de facto stosowanie artykułu 7 lit. a) dyrektywy o ochronie danych.
- wymóg zgody z artykułu 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej (oraz art. 7 lit. a) dyrektywy o ochronie danych) dla reklamy behawioralnej opartej na technikach śledzenia, takich jak pliki Cookies przechowujące informacje w terminalu użytkownika[107].

O ile podstawy prawne są jasne, jeżeli chodzi o art. 5 ust. 3 oraz art. 13 dyrektywy o prywatności i łączności elektronicznej, to nie wszystkie formy marketingu są uwzględnione i pożądane byłoby istnienie wytycznych, w jakich sytuacjach wymagana jest zgoda, o której mowa w art. 7 lit. a) oraz dla których sytuacji osiągnięta jest równowaga na podstawie 7 lit. f), włączając w to możliwość zastosowania mechanizmu opt-out.

W tym aspekcie użyteczne jest przywołanie opinii Grupy Roboczej w sprawie ograniczenia celu, gdzie wprost stwierdzono, że „kiedy organizacja chce konkretnie przeanalizować lub przewidzieć osobiste preferencje, zachowania oraz postawy pojedynczych klientów, co następnie dostarczy informacji „środkom i decyzjom", które są podejmowane wobec tych klientów… wolna, konkretna, świadoma oraz jednoznaczna zgoda „opt-in" prawie na pewno byłaby wymagana, inaczej dalsze przetwarzanie nie zostałoby uznane za zgodne. Co ważne, zgoda taka powinna być wymagana, na przykład, dla celów śledzenia i profilowania na potrzeby marketingu bezpośredniego, reklamy behawioralnej, data-brokeringu (wyszukiwania i udostępniania/sprzedaży danych), reklamy opartej na lokalizacji lub śledzenia opartego na badaniach rynku elektronicznego[108].

[106] Patrz także artykuł 13 ust. 3 dyrektywy o prywatności i łączności elektronicznej, która pozostawia państwom członkowskim wybór między mechanizmem opt-in i opt-out w przypadku marketingu bezpośredniego prowadzonego za pomocą innych sposobów.
[107] W kwestii stosowania tego przepisu patrz opinia 2/2010 Grupy Roboczej w sprawie internetowej reklamy behawioralnej (WP 171).
[108] Patrz Załącznik II (w sprawie Big Data i otwartych danych) opinii (cytowanej w przypisie 9 powyżej), str. 45.

Przyjazne dla prywatności rozwiązania alternatywne w stosunku do „bezpłatnych" usług internetowych

W kontekście, w którym klienci zapisujący się do „bezpłatnych" usług internetowych w rzeczywistości „płacą za" te usługi poprzez pozwalanie na wykorzystanie ich danych osobowych, przyczyniłoby się to również do korzystnej oceny równowagi – lub do zrozumienia, że klient ma rzeczywiste prawo wyboru, i z tego względu przepisy dotyczące ważnej zgody zostały przewidziane w art. 7 lit. f) – jeżeli administrator zaoferował także alternatywną wersję swoich usług, w której „dane osobowe" nie były wykorzystane dla celów marketingowych.

Dopóki takie alternatywne usługi nie będą dostępne, trudniejsza jest argumentacja, że ważna (dobrowolna) zgoda została udzielona zgodnie z art. 7 lit. a) jedynie poprzez wykorzystanie bezpłatnych usług lub że równowaga zgodnie z art. 7 lit. f) powinna być osiągnięta z korzyścią dla administratora.

Powyższe rozważania podkreślają ważną rolę, jaką dodatkowe zabezpieczenia, w tym działający mechanizm opt-out w przypadku przetwarzania, mogą odegrać w zmianie tymczasowej równowagi. Jednocześnie sugerują również, że w niektórych przypadkach art. 7 lit. f) nie może być podstawą przetwarzania, a administratorzy muszą zapewnić ważna zgodę zgodnie z art. 7 lit. a) – lub wypełnić niektóre z warunków dyrektywy – tak aby przetwarzanie miało miejsce.

Możliwość przenoszenia danych, „midata" oraz powiązane kwestie

Wśród dodatkowych zabezpieczeń, które mogą pomóc przechylić równowagę, szczególną uwagę należy poświęcić możliwości przenoszenia danych oraz kwestiom powiązanym, które mogą być coraz bardziej istotne w środowisku internetowym. Grupa Robocza przywołuje swoją Opinię w sprawie ograniczenia celu, w której podkreśliła, że „w wielu sytuacjach środki ochronne, np. te pozwalające osobom, których dane dotyczą/klientom na posiadanie bezpośredniego dostępu do swoich danych w przenośnym, przyjaznym użytkownikowi oraz możliwym do odczytania przez maszyny formacie, może pomóc w nadaniu im uprawnień oraz zaradzić ekonomicznej nierównowadze pomiędzy dużymi korporacjami z jednej strony oraz osobami, których dane dotyczą/klientami z drugiej. Pozwoliłoby to także osobom „korzystać z dobrobytu" stworzonego przez Big Data oraz stanowiłoby bodziec dla przedsiębiorców, aby zaoferowali dodatkowe opcje oraz aplikacje swoim użytkownikom[109].

Dostępność działających mechanizmów dla osób, których dane dotyczą, w celu dostępu do, modyfikacji, usunięcia, przekazania lub dalszego przetwarzania w inny sposób (lub pozwolenia osobom trzecim na dalsze przetwarzanie) swoich własnych danych zapewni uprawnienia osobom, których dane dotyczą, oraz pozwoli im bardziej korzystać z usług

[109] 'Patrz inicjatywy takie jak 'midata' w Zjednoczonym Królestwie, które są oparte na kluczowej zasadzie, że dane powinny być z powrotem udostępniane konsumentom. Midata to dobrowolny program, który z czasem powinien zapewnić konsumentom coraz większy dostęp do ich danych osobowych w przenośnym, elektronicznym formacie. Kluczowy pomysł jest taki, że konsumenci również powinni korzystać z big data poprzez posiadanie dostępu do swoich własnych informacji, aby umożliwić im podejmowanie lepszych wyborów. Patrz także inicjatywy 'Green button' ('Zielony przycisk') , które pozwalają konsumentom na dostęp do informacji nt. ich własnego zużycia energii'. Więcej informacji na temat inicjatyw w Zjednoczonym Królestwie i Francji dostępnych jest na stronie: http//www.midatalab.org.uk/ oraz http://mesinfos.fing.org/.

cyfrowych. Dodatkowo może wpływać na rozwój bardziej konkurencyjnego rynku, poprzez umożliwienie klientom łatwiejszej zmiany dostawców (np. w kontekście bankowości internetowej lub w przypadku dostawców energii w środowisku inteligentnych urządzeń pomiarowych). W końcu, może się także przyczynić do rozwoju dodatkowych, stanowiących wartość dodaną usług przez osoby trzecie, które mogłyby mieć dostęp do danych klientów, na swoją prośbę oraz opierając się na zgodzie konsumentów. Z tej perspektywy możliwość przenoszenia jest nie tylko dobra dla ochrony danych, ale również dla konkurencji oraz ochrony konsumentów[110].

IV. Ustalenia końcowe

W niniejszej opinii Grupa Robocza przeanalizowała kryteria legalności przetwarzania ustanowione w art. 7 dyrektywy. Poza wytycznymi dotyczącymi praktycznej interpretacji oraz stosowania art. 7 lit. f) zgodnie z obowiązującymi ramami prawnymi, jej celem jest sformułowanie zaleceń w celu wspomożenia osób podejmujących decyzje dotyczące polityk w rozważanych przez nich zmianach w obecnych ramach ochrony danych. Przed opracowaniem tych zaleceń, poniżej podsumowano główne ustalenia dotyczące interpretacji art. 7.

IV.1. Wnioski

Przegląd art. 7

Art. 7 wymaga, aby dane osobowe były przetwarzane jedynie wtedy, gdy przynajmniej jedna z sześciu podstaw prawnych wymienionych w tym art. znajduje zastosowanie.

Pierwsza podstawa, art. 7 lit. a), skupia się na zgodzie osoby, której dane dotyczą, jako podstawie legalności. Pozostałe podstawy, przeciwnie, pozwalają na przetwarzanie – z zastrzeżeniem zabezpieczeń – w sytuacjach, gdzie, niezależnie od zgody, odpowiednie i konieczne jest przetwarzanie danych w pewnym kontekście w dążeniu do określonego prawnie uzasadnionego interesu.

Każdy z ustępów b), c), d) oraz e), określa konkretny kontekst, w którym przetwarzanie danych osobowych może być uznane za legalne. Warunki, które znajdują zastosowanie w każdym z tych różnych kontekstów, wymagają dużej uwagi, ponieważ mogą określić zakres różnych podstaw legalności. Konkretnie, kryteria konieczności „dla realizacji umowy", konieczności „dla wykonania zobowiązania prawnego", konieczności „dla ochrony żywotnych interesów osoby, której dane dotyczą" oraz konieczności „dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej" zawierają różne wymogi, które zostały przedyskutowane w Części III.2.

Ustęp f) odnosi się, bardziej ogólnie, do (każdego rodzaju) prawnie uzasadnionego interesu administratora (w jakimkolwiek kontekście). Jednakże ten ogólny przepis poddany jest dodatkowemu testowi równowagi, który wymaga, aby prawnie uzasadnione interesy administratora – lub osoby lub osób trzecich, przed którymi ujawnia się dane – wyważone były względem interesów lub podstawowych praw osób, których dane dotyczą.

[110] W kwestii prawo do przenoszenia danych patrz artykuł 18 projektu rozporządzenia.

Rola art. 7 lit. f)

Art. 7 lit. f) nie powinien być postrzegany jako podstawa prawna, która może być wykorzystana oszczędnie, aby wypełnić luki dotyczące rzadkich oraz nieprzewidzianych sytuacji, „w ostateczności" – lub jako ostania szansa, jeżeli inne podstawy nie mogą być zastosowane. Nie powinna jednakże również być uważana za opcję preferowaną i używana w nadmiernym zakresie, ponieważ byłaby uważana za mniej ograniczającą niż inne podstawy. Raczej, jest tak samo ważna jak każda z pozostałych przesłanek do uprawomocnienia przetwarzania danych osobowych.

Właściwe wykorzystanie art. 7 lit. f) we właściwych okolicznościach oraz przy zastosowaniu odpowiednich zabezpieczeń może pomóc w zapobieganiu wykorzystaniu niezgodnym z przeznaczeniem lub zbyt dużemu poleganiu na innych podstawach prawnych. Odpowiednia ocena równowagi zgodnie z art. 7 lit. f), często z możliwością zastosowania mechanizmu opt-out wobec przetwarzania, może być w niektórych przypadkach ważną alternatywą dla niewłaściwego wykorzystania np. przesłanki „zgody" lub konieczności „dla realizacji umowy". Postrzegany w ten sposób, art. 7 lit. f) stanowi dodatkowe zabezpieczenie w porównaniu do innych z góry określonych podstaw. Nie powinien więc być uznawany za „najsłabsze ogniwo" lub za otwarte drzwi do uprawomocnienia wszystkich czynności przetwarzania danych, które nie podlegają żadnej z innych podstaw prawnych.

Prawnie uzasadnione interesy administratora / interesy lub prawa podstawowe osoby, której dane dotyczą

Pojęcie 'interesu' to szerszy udział, jaki administrator może mieć w przetwarzaniu lub korzyść, jaką odnosi – lub społeczeństwo może odnieść – z przetwarzania. Może to być kuszące, proste lub bardziej kontrowersyjne. Sytuacje, o których mowa w art. 7 lit. f), mogą zatem sięgać od realizacji praw podstawowych czy ochrony ważnych interesów osobistych lub społecznych, aż po inne mniej oczywiste lub nawet problematyczne konteksty.

Aby być uznanym za 'prawnie uzasadniony' i być istotnym na mocy art. 7 lit. f), interes będzie musiał być zgodny z prawem, to jest zgodny z prawem UE i prawem krajowym. Musi być również wystarczająco jasno określony i wystarczająco konkretny, aby pozwolić na przeprowadzenie testu równowagi wobec interesów i praw podstawowych osoby, której dane dotyczą. Musi również stanowić rzeczywisty i obecny interes, tj. nie może być spekulacją.

Jeżeli administrator lub osoba trzecia, którym ujawniono dane, posiada taki prawnie uzasadniony interes, nie oznacza to koniecznie, że może oprzeć się na art. 7 lit. f) jako podstawie prawnej przetwarzania. To, czy można oprzeć się na art. 7 lit. f), będzie zależało od wyniku testu równowagi, który następuje. Przetwarzanie musi także być „konieczne dla celów uzasadnionego interesu administratora" lub – w przypadku ujawnienia – osoby trzeciej. Mniej inwazyjne środki służące temu samemu celowi powinny więc zawsze być preferowane.

Pojęcie „interesu" osób, których dane dotyczą, jest zdefiniowane nawet szerzej, jako że nie wymaga elementu „uzasadnienia". Jeżeli administrator danych lub strona trzecia posiada interes, zakładając, że nie jest on nielegalny, to osoba, której dane dotyczą, jest uprawniona do tego, aby wziąć pod uwagę wszystkie kategorie interesów oraz wyważyć je wobec interesów administratora lub strony trzeciej, o ile są właściwe w zakresie dyrektywy.

Stosowanie testu równowagi

Przy interpretacji zakresu art. 7 lit. f), Grupa Robocza dąży do wyważonego podejścia, które zapewnia konieczną elastyczność administratorom danych w sytuacjach, gdzie nie ma nadmiernego wpływu na osoby, których dane dotyczą, zapewniając jednocześnie wystarczającą pewność prawną oraz gwarancje dla osób, których dane dotyczą, że ten elastyczny przepis nie będzie niewłaściwie wykorzystany.

W celu przeprowadzania testu równowagi ważne jest, aby najpierw rozważyć charakter oraz źródło prawnie uzasadnionego interesu, oraz czy przetwarzanie jest konieczne, aby osiągnąć te interesy z jednej strony, oraz wpływ na osoby, których dane dotyczą, z drugiej. Ta wstępna ocena powinna brać pod uwagę środki, takie jak przejrzystość oraz ograniczone zbieranie danych, które administrator planuje przyjąć, aby zapewnić zgodność z dyrektywą.

Po przeanalizowaniu oraz wyważeniu dwóch stron względem siebie, może być ustanowiona tymczasowa „równowaga": mogą być wyciągnięte wstępne wnioski co do tego, czy prawnie uzasadniony interes administratora będzie nadrzędny wobec praw oraz interesów osób, których dane dotyczą. Mogą jednakże zdarzyć się przypadki, gdzie wynik testu równowagi jest niejasny i istnieją wątpliwości co do tego, czy prawnie uzasadniony interes administratora (lub strony trzeciej) jest nadrzędny oraz czy przetwarzanie może być oparte na art. 7 lit. f).

Z tego powodu ważne jest, aby przeprowadzić dalszą ocenę przy czynnościach wyważania interesów. W tej fazie administrator może uznać, czy jest zdolny do wprowadzenia dodatkowych środków, wykraczających poza zgodność z innymi horyzontalnymi przepisami dyrektywy, tak aby pomóc chronić osoby, których dane dotyczą. Dodatkowe środki mogą obejmować na przykład zapewnianie łatwo działających oraz dostępnych mechanizmów, zapewniających osobom, których dane dotyczą, bezwarunkową możliwość zastosowania mechanizmu opt-out wobec przetwarzania.

Kluczowe czynniki, które należy uwzględnić przy stosowaniu testu równowagi

Opierając się na powyższym, użyteczne czynniki, które należy rozważyć przy przeprowadzaniu testu równowagi obejmują:

- charakter oraz źródło prawnie uzasadnionego interesu, w tym:

  - czy przetwarzanie danych jest konieczne dla realizacji podstawowego prawa, lub
  - w inny sposób leży w interesie publicznym lub cieszy się społecznym, kulturowym lub prawnym/regulacyjnym uznaniem w danej społeczności;

- wpływ na osoby, których dane dotyczą, obejmujący:

  - charakter danych, tj. na przykład, czy przetwarzanie obejmuje dane, które mogą być uznane za wrażliwe lub zostały uzyskane z publicznie dostępnych źródeł;
  - sposób, w jaki dane są przetwarzane, w tym to, czy dane są publicznie ujawnione lub w inny sposób udostępnione dużej liczbie osób, lub czy duża ilość danych osobowych jest przetwarzana lub zestawiana z innymi danych (na przykład w przypadku profilowania, dla celów handlowych, egzekwowania prawa lub innych);
  - racjonalne oczekiwania osoby, której dane dotyczą, szczególnie w odniesieniu do wykorzystania oraz ujawnienia danych w odpowiednim kontekście;
  - status administratora danych oraz osoby, której dane dotycz, obejmujący równowagę sił pomiędzy osobą, której dane dotyczą, oraz administratorem danych, lub czy osoba,

której dane dotyczą jest dzieckiem lub w inny sposób należy do bardziej wrażliwej części społeczeństwa.

- dodatkowe zabezpieczenia w celu zapobieżenia nadmiernemu wpływowi na osoby, których dane dotyczą, obejmujące:

  -minimalizację danych (na przykład ścisłe ograniczenie zbierania danych, lub usunięcie danych natychmiast po wykorzystaniu);
  - środki organizacyjne i techniczne w celu zapewnienia, że dane nie mogą być wykorzystane do podjęcia decyzji lub innych działań w odniesieniu do osób („oddzielenie funkcjonalne");
  - rozległe zastosowanie technik anonimizacyjnych, agregowanie danych, technologie wzmacniające prywatność, prywatność w fazie projektowania, ocena wpływu na prywatność i ochronę danych
  - zwiększona przejrzystość, ogólne oraz bezwarunkowe prawo do mechanizmu opt-out; możliwość przenoszenia danych oraz powiązane środki dające uprawnienia osobom, których dane dotyczą.

Rozliczalność, przejrzystość, prawo do sprzeciwu oraz prawa wykraczające poza nie

W związku z tymi zabezpieczeniami – oraz całościową oceną równowagi – trzy kwestie często odgrywają kluczową rolę w kontekście art. 7 lit. f) i z tego względu wymagają szczególnej uwagi:

- istnienie jakiejś oraz możliwej potrzeby zastosowania dodatkowych środków w celu zwiększenia przejrzystości oraz policzalność;
- prawo osoby, której dane dotyczą, do wyrażenia sprzeciwu wobec przetwarzania, oraz wykraczając poza sprzeciw, dostępność mechanizmu opt-out bez potrzeby jakiegokolwiek uzasadnienia.
- nadanie uprawnień osobie, której dane dotyczą: możliwość przenoszenia danych oraz dostępność działających mechanizmów dla osób, których dane dotyczą: dostępu do, usunięcia, przekazania oraz dalszego przetwarzania w inny sposób (lub umożliwienie dalszego przetwarzania osobom trzecich) ich własnych danych.

IV.2. Zalecenia

Obecne brzmienie art. 7 lit. f) jest elastyczne. Elastyczne słownictwo zostawia dużo miejsca na interpretację i czasami – jak wykazało to doświadczenie – prowadziło do braku przewidywalności oraz braku pewności prawnej. Jednakże, jeżeli jest użyty we właściwym kontekście oraz przy zastosowaniu odpowiednich kryteriów, zgodnie z niniejszą opinią, art. 7 lit. f) ma kluczową rolę do odegrania jako podstawa prawna do legalnego przetwarzania danych osobowych.

Z tego względu Grupa Robocza wspiera obecne podejście zawarte w art. 6 proponowanego rozporządzenia, które utrzymuje równowagę interesów jako odrębną podstawę prawną. Dalsze wytyczne byłyby jednak pożądane, aby zapewnić odpowiednie stosowanie testu równowagi.

Zakres oraz środki do dalszego określenia

Kluczowym wymogiem byłoby, aby przepis pozostawał wystarczająco elastyczny oraz żeby odzwierciedlał obie perspektywy: administratora danych oraz osoby, której dane dotyczą,

oraz dynamiczny charakter określonych kontekstów. Z tego powodu Grupa Robocza uważa, że zapewnienie – w tekście proponowanego Rozporządzenia oraz w aktach delegowanych – szczegółowej oraz wyczerpującej listy sytuacji, w których interes byłby de facto zakwalifikowany jako prawnie uzasadniony nie jest rekomendowane. Grupa Robocza w równym stopniu byłaby przeciwko definiowaniu sytuacji, w których interes lub prawo jednej ze stron powinno *z zasady* lub *z założenia* być nadrzędne wobec interesów lub praw drugiej strony, tylko z powodu charakteru takiego interesu lub prawa, lub z powodu określonych środków ochronnych, które zostały podjęte, na przykład, tego, że dane zostały zaledwie spseudonimizowane. Stanowiłoby to ryzyko zarówno wprowadzenia w błąd, jak i tego, że przepis byłby niepotrzebnie szczegółowy.

Zamiast formułować ostateczne oceny merytoryczne różnych praw oraz interesów, Grupa Robocza nalega na *nadanie kluczowej roli testowi równowagi* w ocenie art. 7 lit. f). Istnieje potrzeba utrzymania elastyczności testu, ale sposób w jaki jest on przeprowadzany, musi być bardziej efektywny w praktyce i musi pozwalać na bardziej skuteczne zapewnienie zgodności. Należy to rozumieć jako *wzmocniony* obowiązek *rozliczalności* administratorów danych, tam gdzie administrator ponosi odpowiedzialność za *wykazanie*, że jego interesy nie są podporządkowane interesom i prawom osób, której dane dotyczą.

Wytyczne oraz rozliczalność

Aby to osiągnąć, Grupa Robocza zaleca, aby wytyczne były przewidziane w proponowanym Rozporządzeniu w następujący sposób.

1) Byłoby pomocne zidentyfikowanie oraz przedstawienie w motywie preambuły niewyczerpującej listy kluczowych elementów do rozważenie, przy zastosowaniu testu równowagi, takich jak charakter oraz źródło prawnie uzasadnionego interesu, wpływ na osoby, których dane dotyczą, oraz dodatkowe zabezpieczenia (środki ochronne), które mają być zastosowane przez administratora w celu zapobieżenia jakiemukolwiek nadmiernemu wpływowi na osoby, których dane dotyczą. Te środki ochronne mogą obejmować m.in.:

    - oddzielenie funkcjonalne danych, odpowiednie wykorzystanie technik anonimizacyjnych, szyfrowanie oraz inne środki organizacyjne i techniczne, w celu ograniczenia potencjalnego ryzyka dla osób, których dane dotyczą;

    - ale również środki w celu zapewnienia zwiększonej przejrzystości oraz wyboru dla osób, których dane dotyczą, takich jak, gdzie to konieczne, możliwości bezwarunkowego zastosowania mechanizmu opt-out wobec przetwarzania, wolnego od opłat oraz w sposób, który może być łatwo oraz skutecznie wywołany.

2) Grupa Robocza wsparłaby również dalsze wyjaśnienie w proponowanym Rozporządzeniu kwestii tego, jak administrator mógłby *wykazać*[111] wzmocnioną rozliczalność.

Zmiana w warunkach skorzystania z prawa do sprzeciwu dla osób, których dane dotyczą, którą przewidziano w art. 19 proponowanego Rozporządzenia jest już ważnym elementem

[111] Takie wykazanie musi być racjonalne i skupić się raczej na wyniku, a nie na procedurze administracyjnej.

rozliczalności. Jeżeli osoby, których dane dotyczą, zgłaszają sprzeciw wobec przetwarzania ich danych osobowych na podstawie art. 7 lit. f), zgodnie z proponowanym Rozporządzeniem to do administratora danych będzie należało wykazanie, że jego interes jest nadrzędny. Odwrócenie ciężaru dowodu jest mocno popierane przez Grupę Roboczą, ponieważ przyczynia się do wzmocnienia obowiązku rozliczalności.

Jeżeli administratorowi danych nie uda się wykazać osobie, której dane dotyczą, w konkretnej sprawie, że jego interes jest nadrzędny, może to także mieć szersze konsekwencje dla całego przetwarzania, nie tylko w odniesieniu do osoby, której dane dotyczą, która zgłosiła sprzeciw. W konsekwencji administrator może zakwestionować lub zreorganizować przetwarzanie, gdy to odpowiednie nie tylko na korzyść konkretnej osoby, której dane dotyczą, ale także z korzyścią dla wszystkich innych osób, których dane dotyczą, które mogą być w podobnej sytuacji[112].

Wymóg ten jest konieczny, ale niewystarczający. Aby zapewnić ochronę od początku oraz uniknąć tego, że zmiana ciężaru dowodu jest obchodzona[113], ważne jest, aby podjąć kroki *przed* rozpoczęciem przetwarzania, a nie tylko w ramach procedury ex-post zgłaszania sprzeciwu. Z tego względu proponuje się, aby na pierwszym etapie jakiegokolwiek przetwarzania administrator danych podjął kilka kroków. Dwa pierwsze kroki mogłyby być wymienione w preambule proponowanego Rozporządzenia, a trzeci w specjalnym artykule:

- *Przeprowadzenie oceny*[114], która powinna zawierać różne etapy analizy rozwiniętej w niniejszej opinii oraz podsumowanej w Załączniku nr 1. Administrator musiałby

[112] Obok odwrócenia ciężaru dowodu, Grupa Robocza popiera także fakt, że projekt rozporządzenia już nie będzie wymagał, aby sprzeciw był wyrażony z '*ważnych* i uzasadnionych przyczyn wynikających z konkretnej sytuacji' [osoby, której dane dotyczą]. Zgodnie z projektem rozporządzenia, wystarczające byłoby raczej odniesienie do wszelkich (niekoniecznie 'ważnych') i uzasadnionych przyczyn wynikających z konkretnej sytuacji osoby, której dane dotyczą. W rzeczywistości kolejną możliwością, która została zaproponowana w Ostatecznym sprawozdaniu Komisji LIBE, jest również pozbycie się wymogu, aby sprzeciw musiałby odnosić się do konkretnej sytuacji osoby, której dane dotyczą. Grupa Robocza popiera to podejście w rozumieniu, że zaleca, aby osoby, których dane dotyczą, były w stanie korzystać albo z jednej albo z obu możliwości, gdy to właściwe, tj., albo z możliwości wyrażenia sprzeciwu w oparciu o ich własną konkretną sytuację, albo w bardziej ogólnym zakresie, a w tym ostatnim przypadku bez wymogu zapewnienia określonego uzasadnienia. W tym rozumieniu patrz poprawka 114 do artykułu 19 ust. 1 w sprawie projektu rozporządzenia w Ostatecznym sprawozdaniu Komisji LIBE.

[113] Administratorzy danych mogą np. mieć pokusę unikania wykazywania dla konkretnych przypadków, że ich interes jest nadrzędny, używając standardowe formy uzasadnienia lub mogą w inny sposób powodować, że korzystanie z prawa do sprzeciwu będzie skomplikowane

[114] Ocena ta, jak wskazano wcześniej w przypisie 84, nie powinna być mylona ze szczegółową oceną wpływu na ochronę prywatności i danych. Obecnie brak jest szczegółowych wytycznych w kwestii ocen wpływu na poziomie europejskim, chociaż w niektórych obszarach, mianowicie w przypadku RFID i inteligentnego opomiarowania, podjęto szereg wysiłków na rzecz zdefiniowania metodologii/ram sektorowych (i/lub szablonu), które mogłyby być stosowane w całej Unii Europejskiej. Patrz 'Propozycja branży dotycząca ram oceny wpływu na ochronę danych i prywatności dla aplikacji RFID' oraz 'Szablon oceny wpływu na ochronę danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych' przygotowany przez grupę ekspertów nr 2 w ramach Grupy zadaniowej Komisji ds. inteligentnych sieci. Grupa Robocza wydała kolejne opinie dotyczące obu tych metodologii.
Ponadto podjęto inicjatywy na rzecz określenia ogólnej metodologii oceny wpływu na ochronę danych, które mogą pomóc w wysiłkach typowych dla tego obszaru. Patrz np. Projekt PIAF (Ramy oceny wpływu na prywatność dla praw ochrony danych i prywatności): http://www.piafproject.due/.
W kwestii wytycznych na poziomie krajowym patrz np. metodologia CNIL:
http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

wyraźnie zidentyfikować przeważające interesy oraz wskazać dlaczego przeważają nad interesami osób, których dane dotyczą. Taka uprzednia ocena nie powinna być zbyt dużym ciężarem oraz pozostać *skalowalna:* może być ograniczona do kluczowych kryteriów, jeżeli wpływ przetwarzania na osoby, których dane dotyczą jest *na pierwszy rzut oka* nieznaczny, podczas gdy z drugiej strony, powinna być przeprowadzona bardziej szczegółowo, jeżeli równowaga byłaby trudna do uzyskania oraz wymagałaby na przykład przyjęcia kilku dodatkowych środków ochronnych. Gdzie to odpowiednie – tj. kiedy operacje przetwarzania stanowią konkretne ryzyko dla praw oraz wolności osób, których dane dotyczą – powinna być przeprowadzona bardziej całościowa ocena wpływu na prywatność oraz na ochronę danych (zgodnie z art. 33 proponowanego Rozporządzenia), której ocena na podstawie art. 7 lit. f) mogłaby być ważną częścią.

- Udokumentowanie tej oceny. Tak jak *skalowalny* jest stopień szczegółowości oceny, której przeprowadzenie jest potrzebne, tak samo zakres dokumentów powinien być skalowalny. Biorąc to pod uwagę, niektóre podstawowe dokumenty powinny być dostępne we wszystkich sprawach, z wyjątkiem najbardziej błahych, niezależnie od oceny wpływu przetwarzania na osobę. To na podstawie takiej dokumentacji ocena administratora może być dalej oceniana i być może zakwestionowana;

- Nadanie przejrzystości oraz widoczności tej informacji dla osób, których dane dotyczą, oraz innych zainteresowanych osób. Przejrzystość powinna być zapewniona zarówno wobec osób, których dane dotyczą oraz organów ochrony danych, jak i gdzie to konieczne, opinii publicznej. Jeżeli chodzi o osoby, których dane dotyczą, Grupa Robocza odwołuje się do projektu sprawozdania Komisji LIBE[115], który stanowi, że administrator powinien poinformować osoby, których dane dotyczą, o powodach dla których wierzy, że jego interesy nie są podporządkowane interesom lub podstawowym prawom i wolnościom osoby, której dane dotyczą. Informacja taka w opinii Grupy Roboczej powinna być przekazana osobie, której dane dotyczą, razem z informacją, którą administrator musi przekazać na podstawie art. 10 oraz 11 obecnej dyrektywy (art. 11 proponowanego Rozporządzenia). Pozwoli to na możliwy sprzeciw osoby, której dane dotyczą, w drugiej fazie oraz na przedstawienie dodatkowego uzasadnienia przez administratora danych w poszczególnych przypadkach wykazującego przeważający interes. Dodatkowo, na wniosek dokumentacja na której administrator oparł ich ocenę powinna być udostępniona organom ochrony danych w celu umożliwienia możliwej weryfikacji oraz wdrożenia, tam gdzie to konieczne.

Grupa Robocza wyraziłaby poparcie, aby te trzy kroki były wyraźnie przewidziane w proponowanym Rozporządzeniu w sposób, w jaki przedstawiono to powyżej. Pozwoliłoby to uznać konkretną rolę podstaw prawnych w ocenie legalności oraz wyjaśniłoby ważność testu równowagi w szerszym kontekście środków rozliczalności oraz ocen wpływu w proponowanych nowych ramach prawnych.

---

oraz Podręcznik ICO dot. wpływu na ochronę prywatności: http://ico.org.uk/pia_handbook_html_v2/files/PIAhanbookV2.pdf.

[115] Projekt raportu w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Grupa Robocza uważa również za wskazane powierzenie EROD zadania zapewnienia dalszych wytycznych tam gdzie to konieczne na podstawie tych ram. Podejście to pozwoliłoby zapewnić zarówno wystarczającą jasność tekstu, jak i wystarczającą elastyczność w jego wdrożeniu.

Załącznik 1. Krótki przewodnik na temat tego, jak przeprowadzić test równowagi na podstawie art. 7 lit. f)

Krok 1: Ocena, która podstawa prawna może potencjalnie znajdować zastosowanie zgodnie z art. 7 lit. a) – f)

Przetwarzanie danych może być zastosowane tylko, jeżeli jedna lub więcej z sześciu podstaw prawnych – od a) do f) – art. 7 znajduje zastosowanie (można oprzeć się na różnych podstawach przy tej samej czynności przetwarzania danych). Jeżeli na pierwszy rzut oka wydaje się, że art. 7 lit. f) może być odpowiedni jako podstawa prawna, proszę przejść do kroku nr 2.

Szybkie porady
- Art. 7 lit. a) znajduje zastosowanie tylko gdy udzielono dobrowolnej, świadomej, konkretnej oraz jednoznacznej zgody; okoliczność, że osoba nie zgłosiła sprzeciwu zgodnie z art. 14, nie powinna być mylona ze zgodą na podstawie art. 7 a) – jednakże łatwy mechanizm złożenia sprzeciwu wobec przetwarzania może być uznany za ważny środek ochronny zgodnie z art. 7 lit. f);
- Art. 7 lit. b) dotyczy przetwarzania, jeżeli jest niezbędne do realizacji umowy; to, że przetwarzanie danych jest związane z umową lub przewidziane gdzieś w warunkach umowy nie oznacza koniecznie, że ta podstawa nie ma zastosowania; gdzie to odpowiednie, proszę rozważyć art. 7 lit. f) jako alternatywę;
- Art. 7 lit. c) dotyczy tylko jasnych oraz konkretnych zobowiązań prawnych zgodnie z prawem UE lub państwa członkowskiego; w przypadku niewiążących wytycznych (np. agencji regulacyjnych) lub zagranicznych zobowiązań prawnych proszę rozważyć art. 7 lit. f) jako alternatywę.

Krok 2: Zakwalifikowanie interesu jako „prawnie uzasadniony" lub „nieuzasadniony"

Aby był uznany za prawnie uzasadniony, interes musi łącznie spełniać następujące obowiązki:
- być zgodny z prawem (tj. zgodny z prawem UE oraz prawem krajowym)
- być wystarczająco jasno wyrażony, tak aby pozwolić na przeprowadzenie testu równowagi względem interesów oraz podstawowych praw i wolności osoby, której dane dotyczą (tj. być wystarczająco konkretny);
- stanowić rzeczywisty i obecny interes (tj. nie spekulatywny)

Krok 3: Określenie czy przetwarzanie jest konieczne do osiągnięcia interesu

Aby spełnić ten wymóg, proszę rozważyć czy nie istnieją inne, mniej inwazyjne środki do osiągnięcia określonego celu przetwarzania oraz służące interesowi administratora danych.

Krok 4: Ustanowienie tymczasowej równowagi przy ocenie, czy interes administratora danych jest podporządkowany podstawowym prawom i wolnościom osoby, której dane dotyczą

- Proszę rozważyć charakter interesów administratora (prawa podstawowe, innego typu interesy, interes publiczny)
- Proszę ocenić możliwe szkody poniesione przez administratora, osoby trzecie lub szerszą społeczność, jeżeli przetwarzanie danych nie będzie miało miejsca;

- Proszę wziąć pod uwagę charakter danych (wrażliwe w węższym czy szerszym sensie?)
- Proszę rozważyć status osoby, której dane dotyczą (nieletni, pracownik, etc.) oraz administratora (na przykład, czy to jest organizacja biznesowa posiadająca dominującą pozycję na rynku);
- Proszę wziąć pod uwagę sposób, w jaki dane są przetwarzane (duża skala, wydobywanie danych, profilowanie, ujawnienie dużej liczbie osób lub publikacja);
-Proszę zidentyfikować podstawowe prawa oraz/lub interesy osoby, której dane dotyczą, na które może być wywarty wpływ;
- Proszę rozważyć racjonalne oczekiwania osoby, której dane dotyczą;
- Proszę ocenić wpływy na osobę, której dane dotyczą, oraz porównać je z oczekiwanymi korzyściami z przetwarzania dla administratora danych.

Szybka porada: Proszę rozważyć efekt rzeczywistego przetwarzania na poszczególne osoby - nie należy uważać tego za abstrakcyjne lub hipotetyczne działanie.

Krok 5: Ustanowienie ostatecznej równowagi biorąc pod uwagę dodatkowe środki ochronne

Proszę zidentyfikować oraz wdrożyć odpowiednie dodatkowe środki ochronne wynikające z obowiązku dochowania należytej staranności, takie jak:
- minimalizacja danych (na przykład ścisłe ograniczenia zbierania danych lub natychmiastowe usunięcie danych po wykorzystaniu);
- środki organizacyjne i techniczne w celu zapewnienia, że dane nie mogą być wykorzystane do podjęcia decyzji lub innych działań w odniesieniu do osób;
- rozległe zastosowanie technik anonimizacyjnych, agregowanie danych, technologie wzmacniające prywatność, prywatność w fazie projektowania, ocena wpływu na prywatność i ochronę danych;
- zwiększona przejrzystość, ogólne oraz bezwarunkowe prawo do mechanizmu opt-out; możliwość przenoszenia danych oraz powiązane środki dające uprawnienia osobom, których dane dotyczą.

Szybka porada: Wykorzystywanie technologii wzmacniających prywatność oraz podejść może przechylić równowagę na korzyść administratora danych a także chronić prywatność osób.

Krok 6: Wykazanie zgodności oraz zapewnienie przejrzystości

- Proszę oprzeć się na krokach od 1 do 5, aby uzasadnić przetwarzanie przed jego rozpoczęciem.
- Proszę poinformować osoby, których dane dotyczą, o powodach wiary w to, że równowaga przechyla się na korzyść administratora;
- Proszę zachować dokumentację, aby była dostępna dla organów ochrony danych.

Szybka porada: Krok ten jest *skalowalny*: szczegółowa ocena oraz dokumentacja powinna być zaadaptowana do charakteru oraz kontekstu przetwarzania. Środki te będą bardziej obszerne, gdy jest przetwarzana duża liczba informacji na temat wielu ludzi, w sposób, który może mieć znaczący wpływ na nich. Całościowa ocena wpływu na prywatność oraz ochronę danych (zgodnie z art. 33 proponowanego Rozporządzenie) będzie konieczna tylko wtedy, gdy operacje przetwarzania stanowią konkretne ryzyko dla praw oraz wolności osób, których

dane dotyczą. W przypadkach tych ocena zgodnie z art. 7 lit. f) może stać się kluczową częścią tej szerszej oceny wpływu.

Krok 7: Co należy uczynić w sytuacji, gdy osoba, której dane dotyczą, korzysta ze swojego prawa do wyrażenia sprzeciwu?

- W sytuacji, gdy dostępne jest jedynie kwalifikowane prawo do zastosowania mechanizmu opt-out jako zabezpieczenia (jest to wprost wymagane zgodnie z art. 14 lit. a) jako minimalne zabezpieczenia): w przypadku gdy osoba, której dane dotyczą zgłasza, sprzeciw wobec przetwarzania, powinno się zapewnić, że zastosowano odpowiedni oraz przyjazny użytkownikowi mechanizm w celu ponownej oceny równowagi zainteresowanych osób oraz wstrzymania przetwarzania ich danych, jeżeli ponowna ocena wykaże, że ich interes jest nadrzędny.
- W sytuacji, gdy zapewniono bezwarunkowe prawo do skorzystania z mechanizmu opt-out jako dodatkowego zabezpieczenia (zarówno ponieważ jest to wprost wymagane w art. 14 lit. b) lub ponieważ z innych względów zostało to uznane za konieczny lub pomocny środek ochronny): w przypadku, gdy osoba, której dane dotyczą, zgłasza sprzeciw wobec przetwarzania, powinno się zapewnić, że ten wybór jest szanowany, bez potrzeby podejmowania dalszych kroków lub oceny.

Załącznik 2. Praktyczne przykłady obrazujące zastosowanie testu równowagi z art. 7 lit. f)

Niniejszy załącznik przedstawia przykłady w odniesieniu do niektórych najczęstszych kontekstów, w których może się pojawić kwestia prawnie uzasadnionego interesu w rozumieniu art. 7 lit. f). W większości przypadków, pogrupowaliśmy dwa lub więcej powiązanych przykładów, które są warte porównania w jednym nagłówku. Wiele przykładów jest opartych na rzeczywistych sprawach lub elementach rzeczywistych spraw, którymi zajmują się organy ochrony danych w różnych państwach członkowskich. Jednakże czasami zmienialiśmy okoliczności do pewnego stopnia, aby pomóc lepiej przedstawić, to jak przeprowadzać test równowagi.

Przykłady zostały załączone, aby zobrazować *proces myślenia* – metodę do wykorzystania przy przyprowadzeniu testu równowagi składającego się z wielu elementów. Innymi słowy, przykłady nie mają zapewnić ostatecznej oceny opisanych spraw. Istotnie, w wielu przypadkach zmiana okoliczności sprawy w jakiś sposób (na przykład, jeżeli administrator przyjmuje dodatkowe wewnętrzne zabezpieczenia, takie jak bardziej kompletna anonimizacja, lepsze zabezpieczenia oraz większa przejrzystość i bardziej realny wybór dla osób, których dane dotyczą), wynik testu równowagi może się zmienić[116].

Powinno to zachęcić administratorów do większej zgodności ze wszystkimi przepisami horyzontalnymi dyrektywy oraz zaoferować dodatkową ochronę, tam gdzie to właściwe opartą na prywatności oraz ochronie danych w fazie projektowania. In większą uwagę administratorzy poświęcają ochronie danych, tym bardziej prawdopodobne, że spełnią wymogi testu równowagi.

Realizacja prawa do wolności wypowiedzi lub informacji[117], w tym w mediach oraz sztuce

Przykład 1: Organizacja pozarządowa ponownie publikuje informacje na temat wydatków członków parlamentu

Organ publiczny publikuje – na skutek obowiązku prawnego (Art. 7 lit. c)) –informacje na temat wydatków członków parlamentu; organizacja pozarządowa zajmująca się przejrzystością natomiast analizuje oraz ponownie publikuje dane w dokładnej, proporcjonalnej oraz lepiej informującej wersji z przypisami, przyczyniając się do większej przejrzystości oraz rozliczalności.

Zakładając, że organizacja pozarządowa przeprowadza ponowną publikację oraz dodaje przypisy w dokładny oraz proporcjonalny sposób, przyjmuje odpowiednie środki ochronne, oraz szerzej, szanuje prawa osób, których sprawa dotyczy, powinna móc oprzeć się na art. 7 lit. f) jako podstawie prawnej przetwarzania. Czynniki takie, jak charakter prawnie uzasadnionego interesu (prawo podstawowe do wolności wypowiedzi lub informacji),

[116] Zastosowanie odpowiednio artykułu 7 lit. f) może podnosić wiele złożonych kwestii dotyczących oceny, a zapewnienie pomocy w ocenie, określone ustawodawstwo, orzecznictwo, wytyczne oraz kodeksy postępowania oraz inne formalne i mniej formalne standardy mogą odgrywać ważną rolę.

[117] W kwestii wolności wypowiedzi lub informacji patrz strona 34 opinii. Przy ocenie tych przykładów należy również wziąć pod uwagę wszelkie istotne wyłączenia w ramach prawa krajowego w przypadku przetwarzania w celach dziennikarskich na mocy artykułu 9 dyrektywy.

publiczny interes w zakresie przejrzystości oraz rozliczalności oraz okoliczność, że dane zostały już ujawnione oraz dotyczą (względnie mniej wrażliwych) danych osobowych związanych z czynnościami osób, dotyczącymi wykonywania ich zadań publicznych[118], przeważają na korzyść zasadności przetwarzania. Okoliczność, że pierwotna publikacja była wymagana przez prawo, oraz że osoby powinny z tego względu oczekiwać, że ich dane będą opublikowane, także przyczynia się do korzystnej oceny. Z drugiej strony równowagi, wpływ na osoby może być znaczący, na przykład z powodu kontroli publicznej uczciwość niektórych jednostek może być kwestionowana i może to prowadzić, na przykład, do porażki w wyborach lub w niektórych przypadkach do śledztw związanych z przestępstwami finansowymi. Powyższe czynniki, rozważane łącznie, wskazują jednakże, że przy wyważaniu interesy administratora (oraz interesy opinii publicznej, której dane są ujawnione) są nadrzędne wobec interesów osób, których dane dotyczą.

Przykład 2: Lokalny radny zatrudnia córkę jako asystenta

Dziennikarz publikuje dokładny, dobrze udokumentowany artykuł w lokalnej gazecie internetowej o lokalnym radnym ujawniającym, że było on obecny jedynie na jednym z ostatnich 11 posiedzeń rady oraz że prawdopodobnie nie zostanie wybrany z uwagi na ostatni skandal związany z zatrudnieniem swojej 17-letniej córki na stanowisku asystenta.

Podobna analiza, jak w przypadku przykładu 1 również znajduje tutaj zastosowanie. Z punktu widzenia okoliczności, opublikowanie informacji jest prawnie uzasadnionym interesem gazety, o której mowa. Mimo że zostały ujawnione dane osobowe dotyczące radnego, podstawowe prawo do wolności wypowiedzi oraz opublikowania historii w gazecie nie jest podporządkowane prawu do prywatności radnego. Jest to spowodowane tym, że prawo do prywatności osób publicznych jest względnie ograniczone w odniesieniu do ich czynności publicznych oraz z uwagi na szczególną ważność wolności wypowiedzi – szczególnie tam, gdzie opublikowana historia dotyczy interesu publicznego.

Przykład 3: Najpopularniejsze wyniki wyszukiwania wciąż pokazują informacje na temat drobnych wykroczeń

Archiwum gazety internetowej zawiera stary artykuł dotyczący jednostki, kiedyś znanej lokalnie osoby, kapitana amatorskiej drużyny futbolowej z małego miasta. Osoba jest zidentyfikowana poprzez podanie pełnego nazwiska oraz opowieści dotyczące względnie nieistotnego przestępstwa (zakłócenie porządku publicznego pod wpływem alkoholu). Dane osoby zostały już usunięte z rejestru karnego, w którym nie figurują już informacje na temat przeszłych przestępstw, za które odbyła karę kilka lat temu. To, co jest najbardziej uciążliwe dla osoby to fakt, że poprzez wyszukiwanie jej nazwiska przy użyciu powszechnie wykorzystywanej wyszukiwarki, link do tej starej informacji pojawia się wśród pierwszych wynikami, które jej dotyczą. Pomimo skierowania przez osobę prośby, gazeta odmówiła przyjęcia środków technicznych, które ograniczyłyby szerszą dostępność informacji na temat

[118] Nie można wykluczyć, że niektóre wydatki mogą ujawnić bardziej wrażliwe dane, takie jak dane dotyczące zdrowia. Jeżeli ma to miejsce, należy je w pierwszym rzędzie usunąć ze zbioru danych przed jego opublikowaniem. Dobrą praktyką jest przyjęcie 'podejścia proaktywnego' oraz zapewnienie osobom możliwości wglądu do ich danych przed publikacją oraz wyraźne informowanie ich o możliwości i metodach publikacji.

osoby, której dane dotyczą. Na przykład gazeta odmówiła przyjęcia środków organizacyjnych oraz technicznych, których celem – w zakresie w jakim pozwala technologia – byłoby ograniczenie dostępu do informacji z zewnętrznych wyszukiwarek, wykorzystujących nazwisko osoby jako kategorię wyszukiwania.

Jest to następna sprawa obrazująca możliwy konflikt pomiędzy wolnością wypowiedzi a ochroną prywatności. Pokazuje także, że w niektórych sprawach dodatkowe zabezpieczenia – takie jak środki zapewniające, że przynajmniej w przypadku uzasadnionego sprzeciwu zgłoszonego na podstawie art. 14 lit. a) dyrektywy odpowiednia część archiwów gazety nie będzie dostępna dla zewnętrznych wyszukiwarek lub format wykorzystywany do wyświetlania informacji nie pozwoli na wyszukiwanie po nazwisku – mogą odegrać kluczową rolę w uzyskaniu odpowiedniej równowagi pomiędzy dwoma zaangażowanymi prawami podstawowymi. Powyższe pozostaje bez żadnego uszczerbku dla innych środków, które mogą być podjęte przez wyszukiwarki internetowe lub inne strony trzecie[119].

Konwencjonalny marketing bezpośredni oraz inne formy marketingu oraz reklamy

Przykład 4: Sklep komputerowy reklamuje podobne produkty wobec klientów

Sklep komputerowy otrzymuje od swoich klientów dane kontaktowe w kontekście sprzedaży produktu oraz wykorzystuje te dane kontaktowe do celów marketingu swoich własnych produktów drogą pocztową. Sklep sprzedaje także produkty w Internecie oraz wysyła promocje pocztą elektroniczną, gdy nowa linia produktów pojawia się w magazynach. Klienci są w jasny sposób informowani o możliwości zgłoszenia w łatwy sposób wolnego od opłat sprzeciwu, kiedy ich dane kontaktowe są zbierane oraz zawsze gdy wysyłana jest wiadomość, jeżeli klient nie wyraził sprzeciwu początkowo.

Przejrzystość przetwarzania, okoliczność, że klient może racjonalnie oczekiwać, że będzie otrzymywać oferty podobnych produktów jako klient sklepu oraz okoliczność, że ma prawo do wyrażenia sprzeciwu, wzmacnia zasadność przetwarzania oraz zabezpiecza prawa osób. Z drugiej strony równowagi nie wydaje się, aby istniał nieproporcjonalny wpływ na prawa osoby do prywatności (w przykładzie tym założyliśmy, że nie istnieją całościowe profile stworzone przez sklep komputerowy dotyczące ich klientów wykorzystujące na przykład szczegółową analizę danych dotyczących kliknięć).

Przykład 5: Apteka internetowa przeprowadza szerokie profilowanie

Apteka internetowa prowadzi marketing oparty na lekach oraz innych produktach, które zostały kupione przez klientów, w tym te na receptę. Analizuje te informacje - zestawiając je z demograficznymi informacjami na temat klientów – na przykład ich wiekiem oraz płcią – aby zbudować profil „dotyczący zdrowia i zamożności" indywidualnych klientów. Wykorzystane są także dane dotyczące kliknięć, które są zbierane nie tylko na temat produktów, które zostały kupione przez klientów, ale także na temat innych produktów oraz informacji, które były wyszukiwane na stronie. Profile klientów obejmują informacje lub przewidywania sugerujące, że określony klient jest w ciąży, cierpi na daną chorobę chroniczną lub byłby zainteresowany zakupem suplementów diety, olejków do opalania lub

[119] Patrz także sprawa c-131/12 Google Spain v Agencia Espanola de Proteccion de Datos, obecnie rozpatrywana przez Trybunał Sprawiedliwości unii Europejskiej.

innych produktów do pielęgnacji skóry, w danym okresie roku. Analitycy internetowej apteki wykorzystują te informacje do oferowania lekarstw nie wydawanych na receptę, suplementów zdrowotnych oraz innych produktów dla określonych osób poprzez pocztę elektroniczną. W tym przypadku apteka nie może opierać się na swoim prawnie uzasadnionym interesie przy tworzeniu oraz wykorzystywaniu profili użytkowników dla celów marketingowych. Istnieje kilka problemów związanych z opisanym profilowaniem. Informacje są szczególnie wrażliwe i mogą ujawniać wiele na temat spraw, co do których osoby mogłyby oczekiwać, że pozostaną prywatne[120]. Zakres oraz sposób profilowania (wykorzystanie danych dotyczących kliknięć, przewidujące algorytmy) także sugeruje wysoki poziom inwazyjności. Zgoda oparta na art. 7 lit. a) oraz art. 8 ust. 2 lit. a) (jeżeli dochodzi do przetwarzania danych wrażliwych) mogłaby jednakże być uznana za alternatywę, tam gdzie to odpowiednie.

Niezamówione informacje niekomercyjne, obejmujące informację dla potrzeb kampanii politycznych oraz zbierania środków na cele charytatywne

Przykład 6: Kandydat w wyborach lokalnych wykorzystuje w ukierunkowany sposób spis wyborców

Kandydat w wyborach lokalnych wykorzystuje spis wyborców[121], aby wysłać list promujący jego kampanię w nadchodzących wyborach do każdego potencjalnego wyborcy w swoim okręgu wyborczym. Kandydat wykorzystuje dane uzyskane ze spisu wyborców jedynie do wysłania listu i nie zatrzymuje danych po zakończeniu kampanii.

Takie wykorzystanie lokalnego spisu mieści się w zakresie racjonalnych oczekiwań osób, jeżeli odbywa się w okresie przedwyborczym: interes administratora jest jasny oraz prawnie uzasadniony. Ograniczone oraz ukierunkowane wykorzystanie informacji także przyczynia się do przechylenia równowagi na korzyść prawnie uzasadnionego interesu administratora. Takie wykorzystanie spisu wyborców może być również regulowane przez prawo na poziomie krajowym, w interesie publicznym, zakładając istnienie konkretnych reguł, ograniczeń oraz środków ochronnych w odniesieniu do wykorzystania spisu wyborców. Jeżeli ma to miejsce, zgodność z tymi konkretnymi regułami jest także wymagana do zapewnienia zasadności przetwarzania.

Przykład 7: Podmiot typu non-profit zbiera informacje do ukierunkowanych celów

Organizacja filozoficzna zajmująca się rozwojem człowieka oraz społeczeństwa zdecydowała się zorganizować zbieranie funduszy oparte na profilowaniu swoich członków. W tym celu zbiera dane dotyczące portali społecznościwych poprzez oprogramowanie ad-hoc skierowane do osób, które „lubią" stronę organizacji, „lubią" lub „dzielą się" wiadomościami organizacji umieszczonymi na jej stronie, regularnie oglądają pewne elementy lub przekazują dalej tweety, umieszczone przez organizację. Następnie wysyła wiadomości oraz newsletter do swoich członków, na podstawie ich profilów. Na przykład starszy właściciel psa, który „polubił" artykuł o schroniskach dla psów, otrzymuje inną prośbę o przekazanie pieniędzy od rodzin z małymi

[120] Poza wszelkimi ograniczeniami stawianymi przez przepisy o ochronie danych, reklamowanie produktów na receptę jest również ściśle uregulowane w UE, i istnieją także określone ograniczenia dotyczące reklamowania leków bez recepty. Ponadto wymóg artykułu 8 dotyczący szczególnych kategorii danych (takich jak dane dotyczące zdrowia) również musi być uwzględniony.

[121] Zakłada się, że w kraju członkowskim, w którym ten przykład ma miejsce, zbiór wyborczy jest ustanowiony na mocy prawa.

dziećmi; osoby z różnych grup etnicznych także otrzymują inne wiadomości.

Okoliczność, że szczególne kategorie danych są przetwarzane (przekonania filozoficzne) wymaga zapewnienia zgodności z art. 8, warunku, który wydaje się być spełniony, ponieważ przetwarzanie odbywa się w ramach prawnie uzasadnionych działań organizacji. Jednak nie jest to wystarczający warunek w tej sprawie: sposób, w jaki dane są wykorzystywane, wykracza poza racjonalne oczekiwania osób. Ilość zbieranych danych, brak przejrzystości na temat zbierania oraz ponownego wykorzystywania danych opublikowanych pierwotnie dla jednego celu w innym celu przyczynia się do stwierdzenia, że nie można oprzeć się na art. 7 lit. f) w tym przypadku. ż tego względu przetwarzanie nie powinno być dozwolone, z wyjątkiem sytuacji, gdy może być wykorzystana inna podstawa, na przykład zgoda osób na podstawie art. 7 lit. a)

Egzekwowanie roszczeń prawnych, w tym to windykacja długów poprzez procedury pozasądowe

Przykład 8: Spór o jakość prac remontowych

Klient prowadzi spór o jakość prac remontowych w kuchni i odmawia zapłacenia pełnej ceny. Firma budowlana przekazuje odpowiednie oraz proporcjonalne dane swojemu prawnikowi, aby mógł przypomnieć klientowi o płatnościach i negocjować ugodę z klientem, jeżeli ciągle będzie odmawiał uiszczenia płatności.

W tej sprawie wstępne kroki podjęte przez firmę budowlaną wykorzystującą podstawowe informacje na temat osoby, której dane dotyczą (na przykład nazwisko, adres, dane kontaktowe) w celu przesłania przypomnienia osobie, której dane dotyczą (bezpośrednio lub poprzez swojego prawnika, tak jak w tej sprawie) mogą ciągle mieścić się w zakresie przetwarzania koniecznego dla realizacji umowy (art. 7 lit. b)). Dalsze kroki[122], w tym zaangażowanie firmy windykacyjnej, powinny być jednakże ocenione na podstawie art. 7 lit. f), biorąc pod uwagę m. in. ich inwazyjność oraz wpływ na osobę, której dane dotyczą, jak to zostanie pokazane w następnym przykładzie.

Przykład 9: Klient znika z samochodem zakupionym na kredyt

Klient nie płaci odsetek, które są wynikiem zakupu drogiego sportowego auta, po czym „znika". Sprzedawca samochodowy wynajmuje osobę trzecią, tj. „firmę windykacyjną". Firma windykacyjna przeprowadza inwazyjne dochodzenie „w stylu egzekwowania prawa", wykorzystując m.in. takie działania, jak ukryty nadzór wideo i podsłuch.

Chociaż interesy sprzedawcy samochodów oraz firmy windykacyjnej są prawnie uzasadnione, równowaga nie przechyla się na ich korzyść z uwagi na inwazyjne metody wykorzystane do zebrania informacji, z których niektóre są wprost zabronione przez prawo (podsłuch). Wniosek byłby inny, jeżeli na przykład sprzedawca samochodów oraz firma windykacyjna przeprowadzają jedynie ograniczone sprawdzenie danych kontaktowych osoby, której dane dotyczą, w celu rozpoczęcia postępowania sądowego.

[122] Obecnie w różnych państwach członkowskich istnieje określony stopień różnorodności, do którego środki mogą być uznane za konieczne do realizacji umowy.

Zapobieganie malwersacjom, korzystaniu z usług niezgodnie z przeznaczeniem oraz praniu pieniędzy

Przykład 10: Weryfikacja danych klienta przed otworzeniem konta bankowego

Instytucja finansowa działa zgodnie z rozsądnymi oraz proporcjonalnymi procedurami – jak niewiążące wytyczne rządowego organu nadzoru finansowego – w celu weryfikacji tożsamości jakiejkolwiek osoby, która chce otworzyć konto. Prowadzi rejestr informacji wykorzystywanych do weryfikacji tożsamości osoby.

Interes administratora jest prawnie uzasadniony, przetwarzanie danych obejmuje jedynie ograniczone oraz konieczne informacje (standardowe działanie w przemyśle, racjonalnie oczekiwane przez osoby, których dane dotyczą oraz zalecane przez właściwe instytucje). Odpowiednie środki ochronne są zastosowane w celu ograniczenia wszelkiego nieproporcjonalnego oraz nadmiernego wpływu na osoby, których dane dotyczą. Administrator może więc oprzeć się na art. 7 lit. f). Alternatywnie oraz w zakresie, w jakim podjęte działania są wymagane szczególnie przez prawo właściwe, może mieć zastosowanie art. 7 lit. c).

Przykład 11: Wymiana informacji w celu zwalczania prania pieniędzy

Instytucja finansowa – po otrzymaniu porady od właściwego organu ochrony danych – wdraża procedurę opartą na konkretnych oraz ograniczonych kryteriach wymiany danych dotyczących podejrzewanego naruszenia reguł przeciwdziałania praniu pieniędzy, z innymi firmami w tej samej grupie, ze ścisłym ograniczeniem dostępu, nadzorem oraz zabronieniem dalszego przetwarzania dla innych celów.

Z powodów podobnych jak te wyjaśnione powyżej oraz w zależności od okoliczności sprawy, przetwarzanie danych może być oparte na art. 7 lit. f). Alternatywnie oraz w zakresie, w jakim działania te są wymagane szczególnie przez prawo właściwe, art. 7 c) może mieć zastosowanie art. 7 lit. c).

Przykład 12: Czarna lista agresywnych osób uzależnionych od narkotyków

Grupa szpitali stworzyła wspólną czarną listę „agresywnych" osób poszukujących narkotyków, w celu zabronienia im dostępu do wszystkich pomieszczeń medycznych zaangażowanych szpitali.

Nawet jeżeli interes administratorów w utrzymaniu bezpieczeństwa pomieszczeń jest prawnie uzasadniony, musi być wyważony względem podstawowego prawa do prywatności oraz innych ważnych kwestii, takich jak potrzeba nie wykluczenia dostępu zainteresowanych osób do leczenia. Okoliczność, że przetwarzane są dane wrażliwe (na przykład dane dotyczące zdrowia związane z uzależnieniem od narkotyków), także wspiera konkluzję, że w tej spawie istnieje małe prawdopodobieństwo, że przetwarzanie byłoby akceptowalne na podstawie art. 7 lit. f)[123]. Przetwarzanie mogłoby być akceptowalne na przykład, jeżeli byłoby regulowane przez prawo przewidujące konkretne środki ochronne (sprawdzanie oraz

[123] Wymogi artykułu 8 dotyczące szczególnych kategorii danych (takich jak dane dotyczące zdrowia) również powinny być uwzględnione.

kontrolę, przejrzystość, zapobieganie zautomatyzowanym decyzjom), zapewniające, że nie skutkowałoby dyskryminacją lub naruszeniem podstawowych praw osób[124]. W ostatnim przypadku, w zależności od tego czy konkretne prawo wymaga czy tylko pozwala na przetwarzanie, można się oprzeć na art. 7 lit. c) lub 7 lit. a) jako na podstawie prawnej.

Monitorowanie pracowników dla celów bezpieczeństwa oraz zarządzania

Przykład 13: Godziny pracy prawników wykorzystane zarówno dla celów rachunkowych, jak i nagród

Liczba fakturowanych godzin przepracowanych przez prawników w kancelariach jest przetwarzana zarówno dla celów rachunkowych, jak i dla określenia rocznych nagród. System jest przejrzyście wytłumaczony pracownikom, którzy mają wyraźne prawo do wyrażenia braku zgody, zarówno dla celów rachunkowych, jak i wypłaty nagród, w którym to przypadku rozmawiają o tym z kadrą zarządzającą.

Przetwarzanie wydaje się konieczne dla prawnie uzasadnionych interesów administratora i nie wydaje się, aby istniała mniej inwazyjna droga do osiągnięcia tego celu. Wpływ na pracowników jest także ograniczony, w wyniku zastosowanych środków ochronnych oraz procedur. Art. 7 lit. f) może być więc odpowiednią podstawą prawną w tej sprawie. Można także argumentować, że przetwarzanie dla jednego lub obu powyższych celów jest także konieczne dla realizacji umowy.

Przykład 14: Elektroniczne monitorowanie wykorzystania Internetu[125]

Pracodawca monitoruje wykorzystanie Internetu podczas godzin pracy przez pracowników, w celu sprawdzenia, czy nie wykorzystują w nadmierny sposób komputerów firmy dla celów prywatnych. Zbierane dane obejmują pliki tymczasowe oraz pliki Cookies generowane na komputerach pracowników, pokazujące odwiedzone strony oraz pliki pobrane podczas godzin pracy. Dane są przetwarzane bez uprzedniej konsultacji z osobami, których dane dotyczą oraz przedstawicielami związków zawodowych/rady pracowniczej w firmie. Nie zapewniono także wystarczającej informacji zainteresowanym osobom o tych praktykach.

Ilość oraz charakter zebranych danych stanowi znaczące naruszenie życia prywatnego pracowników. Dodatkowo kwestia proporcjonalności, przejrzystości działań, ściśle powiązana z racjonalnymi oczekiwaniami osób, których dane dotyczą, jest również istotnym elementem do rozważenia. Nawet jeżeli pracodawca posiada prawnie uzasadniony interes w ograniczaniu czasu spędzanego przez pracowników na odwiedzaniu stron internetowych nie związanych bezpośrednio z ich pracą, zastosowane metody nie spełniają testu równowagi z art. 7 lit. f). Pracodawca powinien wykorzystywać mniej inwazyjne metody (na przykład ograniczanie dostępu do pewnych stron), które są, jako dobra praktyka, omawiane i uzgadniane z przedstawicielami pracowników oraz komunikowane pracownikom w przejrzysty sposób.

Systemy informowania o nieprawidłowościach

[124] Patrz Dokument roboczy w sprawie czarnych list (WP 65) przyjęty 3 października 2002 r.

[125] Kilka państw członkowskich uważa, że określony ograniczony monitoring elektroniczny może być 'konieczny dla realizacji umowy', i w związku z tym może być oparty raczej na podstawie prawnej z artykułu 7 lit. b, a nie art. 7 lit. f).

Przykład 15: System informowania o nieprawidłowościach w celu zapewniania zgodności z zagranicznymi zobowiązaniami prawnymi

Europejski oddział grupy z USA ustanawia ograniczony system informowania o nieprawidłowościach w celu raportowania poważnych naruszeń w dziedzinie rachunkowości oraz finansów. Podmioty z grupy podlegają kodeksowi dobrego zarządzania, który wzywa do wzmocnienia procedur wewnętrznej kontroli oraz zarządzania ryzykiem. Z powodu swoich międzynarodowych działań, od oddziału z UE wymagane jest dostarczanie wiarygodnych danych finansowych innym członkom grupy w USA. Ten system jest zaprojektowany, aby zapewnić zgodność zarówno z prawem UE, jak i z wytycznymi wydanymi przez krajowe organy ochrony danych w UE.

Wśród środków ochronnych pracownikom dano jasne wytyczne dotyczące okoliczności, w których system może być wykorzystany, poprzez szkolenia lub inne środki. Pracownicy zostali ostrzeżeni, żeby nie wykorzystywali systemu niewłaściwie – na przykład poprzez zgłaszanie fałszywych lub niepotwierdzonych oskarżeń przeciwko członkom załogi. Wyjaśniono im także, że jeżeli wolą, mogą korzystać z systemu anonimowo lub jeżeli chcą, mogą się ujawnić. W tej ostatniej sytuacji pracownicy są informowani o okolicznościach, w których informacje ich identyfikujące będą z powrotem przekazane ich pracodawcy lub przekazane innemu podmiotowi.

Jeżeli ustanowienie systemu było wymagane przez prawo UE lub prawo jednego z państw członkowskich, przetwarzanie mogłoby opierać się na art. 7 lit. c). Jednakże zagraniczne zobowiązania prawne nie kwalifikują się jako obowiązek prawny dla celów art. 7 lit. c) i z tego względu takie zobowiązanie nie mogłoby uprawomocniać przetwarzania na podstawie art. 7 lit. c). Jednakże przetwarzanie mogłoby być oparte na art. 7 lit. f), na przykład jeżeli istnieje prawnie uzasadniony interes w zakresie zagwarantowania stabilności rynków finansowych lub walki z korupcją, oraz przy założeniu, że system zawiera odpowiednie zabezpieczenia zgodne z wytycznymi odpowiednich instytucji regulacyjnych w UE.

Przykład 16 „Wewnętrzny" system informowania o nieprawidłowościach bez spójnej procedury

Firma zajmująca się świadczeniem usług finansowych decyduje się na ustanowienie systemu informowania o nieprawidłowościach, ponieważ podejrzewa rozprzestrzenianie się kradzieży oraz korupcji wśród załogi i chce zachęcić pracowników do informowania o obu tych kwestiach. W celu zaoszczędzenia pieniędzy firma decyduje się ustanowić wewnętrzny system, obsadzony przez pracowników departamentu zasobów ludzkich. Aby zachęcić pracowników do wykorzystywania systemu, oferuje nagrody pieniężne „bez zadawania pytań" pracownikom, których działania związane z informowaniem o nieprawidłowościach doprowadziły do wykrycia nieodpowiedniego zachowania oraz odzyskania pieniędzy.

Firma ma prawnie uzasadniony interes w zakresie wykrywania oraz przeciwdziałania kradzieżom oraz korupcji. Jednakże jej system informowania o nieprawidłowościach jest tak źle zaprojektowany i pozbawiony zabezpieczeń, że jej interesy są podporządkowane zarówno interesom, jak i prawom do prywatności jej pracowników – szczególnie tych, którzy mogą być ofiarami fałszywego raportowania złożonego tylko dla korzyści finansowej. Okoliczność, że system jest zarządzany wewnątrz zamiast przez niezależną instytucję, jest tutaj kolejnym problemem, podobnie jak brak szkoleń oraz wytycznych w zakresie wykorzystania systemu.

Bezpieczeństwo fizyczne, informatyczne oraz sieciowe

Przykład 17: Środki kontroli biometrycznej w laboratorium badawczym

Laboratorium badań naukowych pracujące nad zabójczymi wirusami wykorzystuje biometryczny system wejść w związku z wysokim ryzykiem dla zdrowia publicznego w przypadku, gdyby wirusy wydostały się z pomieszczeń. Zastosowano odpowiednie środki ochronne, włączając okoliczność, że dane biometryczne są przechowywane na osobistych kartach pracowników, a nie w scentralizowanym systemie.

Nawet jeżeli dane są wrażliwe w szerokim sensie, powód ich przetwarzania jest w interesie publicznym. To oraz okoliczność, że ryzyka wykorzystania niezgodnie z przeznaczeniem ą zredukowane przez odpowiednie środki ochronne czyni art. 7 lit. f) odpowiednią podstawą przetwarzania.

Przykład 18: Ukryte kamery w celu identyfikacji palących gości oraz pracowników

Firma używa ukrytych kamer w celu identyfikacji pracowników oraz gości, którzy palą w nieprzeznaczonych do tego strefach w budynku.

Chociaż administrator ma prawnie uzasadniony interes w zapewnieniu zgodności z regułami dotyczącymi zakazu palenia, środki wykorzystane do osiągnięcia tego celu są – ogólnie mówiąc – nieproporcjonalne i niepotrzebnie inwazyjne. Istnieją mniej inwazyjne i bardziej przejrzyste metody (takie jak czujniki dymu czy widoczne znaki), które są dostępne. Zatem przetwarzanie nie zapewnia zgodności z art. 6, który wymaga, aby dane nie były nadmierne w odniesieniu do celów, dla których są zbierane lub dalej przetwarzane. Jednocześnie nie spełnia również prawdopodobnie wymogów testu równowagi zgodnie z art. 7.

Badania naukowe

Przykład 19: Badania dotyczące wpływu rozwodu oraz bezrobocia rodziców na osiągnięcia edukacyjne dzieci

Zgodnie z programem badawczym przyjętym przez rząd oraz za zgodą właściwego komitetu ds. etyki badania są przeprowadzane odnośnie relacji pomiędzy rozwodami, bezrobociem rodziców oraz osiągnięciami edukacyjnymi dzieci. Chociaż informacje te nie są klasyfikowane jako „szczególne kategorie danych", badanie skupia się na kwestiach, które dla wielu rodzin byłyby bardzo intymnymi informacjami. Badania pozwolą na specjalną pomoc edukacyjną dla wybranych dzieci, które w innym przypadku mogą przestać przychodzić na zajęcia, osiągać słabe wyniki w edukacji, popaść w wieku dorosłym w bezrobocie lub zająć się działalnością przestępczą. Prawo zainteresowanych państw członkowskich wyraźnie zezwala na przetwarzanie danych osobowych (innych niż szczególne kategorie danych) dla celów badawczych, jeżeli badania są konieczne dla ważnego interesu publicznego oraz wykonywane przy zastosowaniu odpowiednich środków ochronnych, które są następnie bardziej szczegółowo określone w prawie wykonawczym. Te ramy prawne zawierają specjalne wymogi, ale również ramy rozliczalności, które pozwalają na ocenę w poszczególnych przypadkach dopuszczalności badań (jeżeli są przeprowadzane bez zgody osób, których dane dotyczą) oraz specjalne środki do zastosowania, aby chronić osoby, których dane dotyczą.

Badacz prowadzi zapewniający bezpieczeństwo instytut badań oraz, zgodnie z warunkami bezpieczeństwa, właściwe informacje są mu przekazywane z rejestrów ludności, sądów, agencji bezrobocia oraz szkół. Centrum badawcze wykorzystuje „funkcje skrótu" do badań nad tożsamością „osób", tak że dane dotyczące rozwodów, bezrobocia oraz ocen w edukacji mogą być połączone, ale bez ujawniania „cywilnej" tożsamości jednostek – na przykład ich nazwisk i adresów. Wszystkie pierwotne dane są nieodwracalnie usunięte. Podejmowane są także dalsze środki, zapewnić odrębność funkcjonalną (tj. dane będą wykorzystane tylko dla celów badawczych) oraz zredukowanie jakiegokolwiek dalszego ryzyka ponownej identyfikacji.

Członkowie załogi pracującej w centrum badawczym otrzymują rygorystyczne szkolenia w zakresie bezpieczeństwa oraz są osobiście - prawdopodobnie nawet karnie – odpowiedzialni za wszelkie naruszenia ochrony danych, za które są odpowiedzialni. Podjęte są środki techniczne oraz organizacyjne, na przykład w celu zapewnienia, że załoga wykorzystująca klucze USB nie mogą usunąć danych osobowych z centrum.

Prowadzenie badań przez centrum badawcze leży w jego prawnie uzasadnionym interesem, jeżeli występuje ważny interes publiczny tych badań. Jest także prawnie uzasadnionym interesem pracodawcy, podmiotów edukacyjnych oraz innych podmiotów zaangażowanych w system, ponieważ pomaga im zaplanować oraz dostarczyć usługi tym, którzy najbardziej ich potrzebują. Aspekty prywatności systemu zostały dobrze zaprojektowane, a zastosowane środki ochronne oznaczają, że prawnie uzasadniony interes organizacji zaangażowanych w prowadzenie badań nie jest podporządkowany ani interesom ani prawu do prywatności rodziców lub dzieci, których dane stanowią podstawę badań.

Przykład 20: Badania naukowe na temat otyłości

Uniwersytet chce przeprowadzić badania na temat poziomu otyłości dzieci w kilku miastach i rejonach wiejskich. Pomimo ogólnych trudności w uzyskaniu dostępu do odpowiednich danych ze szkół oraz innych instytucji, udało mu się przekonać kilkudziesięciu nauczycieli do monitorowania przez pewien czas dzieci w ich klasach, które wydają się otyłe oraz pytania ich o ich dietę, stopień aktywności fizycznej, grania w gry komputerowe itp. Nauczyciele ci rejestrują także nazwiska oraz adresy przepytanych dzieci, tak aby móc przesłać im voucher na muzykę w Internecie, jako nagrodę za udział w badaniach. Naukowcy zestawiają także bazy danych na temat dzieci, zestawiających poziomy otyłości z aktywnością fizyczną oraz innymi elementami. Kopie papierowe kompletnych wywiadów – ciągle w formie identyfikującej poszczególne dzieci – są przechowywane w archiwach uniwersytetu, przez nieokreślony czas oraz bez odpowiednich środków ochronnych. Kopie papierowe wszystkich kwestionariuszy są udostępniane na prośbę jakimkolwiek studentom studiów magisterskich lub doktoranckich tego samego lub partnerskiego uniwersytetu na świecie, którzy wykażą zainteresowanie wykorzystaniem danych badawczych.

Chociaż przeprowadzenie badań jest prawnie uzasadnionym interesem uniwersytetu, istnieje kilka aspektów projektu badań oznaczających, że interesy te są podporządkowane interesom oraz prawu do prywatności dzieci. Poza metodologią badań, której brakuje rygoru naukowego, problem wynika w szczególności z braku podejścia wzmacniającego prywatność w projekcie badań oraz szerokiego dostępu do zebranych danych osobowych. W żadnym momencie dane dzieci nie są kodowane lub anonimizowane, a także nie podjęto innych środków w celu zapewnienia bezpieczeństwa lub funkcjonalnej odrębności danych. Ważne

zgody zgodnie z art. 7 lit. a) oraz 8 ust. 2 lit. a) nie zostały uzyskane i nie jest jasne czy wyjaśniono dzieciom lub ich rodzicom, do czego będą używane ich dane oraz z kim będą dzielone.

Zagraniczne zobowiązania prawne

Przykład 21: Zapewnienie zgodności z wymogami prawa podatkowego państwa trzeciego

Banki z UE zbierają oraz przekazują niektóre dane swoich klientów dla celów zapewnienia zgodności z obowiązkami podatkowymi w państwie trzecim. Zbieranie oraz przekazywanie jest określone oraz odbywa się zgodnie z obowiązkami i środkami ochronnymi uzgodnionymi pomiędzy UE oraz innym krajem w umowie międzynarodowej.

Chociaż zagraniczne obowiązki nie mogą jako takie być uzasadnioną podstawą przetwarzania zgodnie z art. 7 lit. c), mogą nimi być, jeżeli taki obowiązek jest podtrzymany w umowie międzynarodowej. W tej ostatniej sytuacji przetwarzanie może być uznane za konieczne dla zapewnienia zgodności z zobowiązaniami prawnymi inkorporowanymi do wewnętrznych ram prawnych w umowie międzynarodowej. Jednakże jeżeli nie ma takiej umowy, zbieranie oraz przekazywanie będzie musiało być ocenione w odniesieniu do wymogów art. 7 lit. f) oraz może być uznane za dopuszczalne tylko, jeżeli zapewniono odpowiednie środki ochronne, jak te zaaprobowane przez odpowiedni organ ochrony danych (zobacz także *przykład 15* powyżej)

Przykład 22: Przekazywanie danych dysydentów

Na wniosek, firma z UE przekazuje dane zagranicznych rezydentów do państwa trzeciego, w którym istnieje opresyjny reżim, które chce dostępu do danych dysydentów (na przykład dane dotyczące przepływu poczty elektronicznej, zawartość poczty elektronicznej, historia wyszukiwania lub wiadomości prywatne w sieciach społecznościowych).

W tym przypadku, inaczej niż w poprzednim, nie ma umowy międzynarodowej, która pozwalałaby na zastosowanie art. 7 lit. c) jako podstawy prawnej. Poza tym kilka elementów powoduje, że art. 7 lit. f) nie byłby odpowiednią podstawą przetwarzania. Chociaż administrator może mieć interes ekonomiczny w zapewnieniu, że spełnia prośby zagranicznego rządu (inaczej mógłby być poddany mniej korzystnemu traktowaniu przez rząd państwa trzeciego w porównaniu do innych firm), zgodność z prawem oraz proporcjonalność przekazania jest mocno wątpliwa, zgodnie z ramami prawnymi praw podstawowych UE. Potencjalnie ogromny wpływ na zainteresowane osoby (na przykład dyskryminacja, uwięzienie, kara śmierci) także w ogromnym stopniu stanowi na korzyść interesów oraz praw zainteresowanych osób.

Ponowne wykorzystanie publicznie dostępnych danych

Przykład 23: Ocena polityków[126]

Organizacja pozarządowa wykorzystuje publicznie dostępne dane polityków (obietnice

[126] Patrz i porównaj także z przykładem 7 powyżej.

złożone w czasie wyborów oraz faktyczna historia głosowania) w celu ich oceny na podstawie tego, jak dobrze wywiązują się z obietnic.

Nawet jeżeli wpływ na zainteresowanych polityków może być znaczący, okoliczność, że przetwarzanie jest oparte na informacji publicznej oraz związane z ich obowiązkami publicznymi powoduje, z jasnym celem wzmocnienia przejrzystości oraz rozliczalności, przechylenie równowagi w interesie administratora[127].

Dzieci oraz inne podatne osoby

Przykład 24: Internetowe strony informacyjne dla nastolatków

Strona internetowa organizacji pozarządowej oferująca nastolatkom porady w kwestiach związanych z uzależnieniem od narkotyków, niechcianą ciążą oraz uzależnieniem od alkoholu zbiera poprzez swój własny serwer dane o gościach strony. Następnie natychmiast anonimizuje dane oraz przekształca je w ogólną statystykę dotyczącą tego, która część strony jest najbardziej popularna wśród gości pochodzących z różnych regionów geograficznych kraju.

Art. 7 lit. f) może być wykorzystany jako podstawa prawna, nawet jeżeli dane dotyczące podatnych osób są zaangażowane, ponieważ przetwarzanie odbywa się w interesie publicznym oraz zastosowane są ścisłe środki ochronne (dane są anonimizowane natychmiast oraz wykorzystane tylko do utworzenia statystyki), co pomaga przechylić szalę na korzyść administratora.

Rozwiązania dotyczące ochrony prywatności w fazie projektowania jako dodatkowe zabezpieczenia

Przykład 25: Dostęp do numerów telefonów komórkowych użytkowników oraz osób niebędących użytkownikami aplikacji „porównaj i zapomnij"

Dane osobowe osób są przetwarzane w celu sprawdzenia, czy udzieliły już jednoznacznej zgody w przeszłości (tj. „porównaj oraz zapomnij" jako środek ochronny).

Od twórcy aplikacji wymaga się, aby posiadał jednoznaczną zgodę osób, których dane dotyczą, na przetwarzanie ich danych osobowych: na przykład twórca aplikacji, który chce uzyskać dostęp oraz zbierać całe elektroniczne książki adresowe użytkowników aplikacji, w tym numery telefonów komórkowych osób zapisanych w kontaktach, które nie wykorzystują aplikacji. Aby móc to zrobić, najpierw musiałby ocenić, czy właściciele numerów telefonów komórkowych w książkach adresowych użytkowników aplikacji udzieliły swojej jednoznacznej zgody (zgodnie z art. 7 lit. a) na przetwarzanie ich danych.

Dla tego ograniczonego początkowego przetwarzania (tj. krótkoterminowego dostępu do pełnej książki adresowej użytkownika aplikacji), twórca aplikacji może oprzeć się na art. 7 lit. f) jako podstawie prawnej, przy zastosowaniu środków ochronnych. Te środki ochronne powinny zawierać środki techniczne oraz organizacyjne w celu zapewnienia, że firma

[127] Podobnie jak w przykładach 1 i 2, założyliśmy, ze publikacja jest prawidłowa i proporcjonalna – brak zabezpieczeń i inne czynniki mogą zmienić równowagę interesów w zależności od okoliczności sprawy.

wykorzystuje ten dostęp tylko, aby pomóc użytkownikowi zidentyfikować, które z osób, do których ma kontakt, są już użytkownikami i które z tego powodu udzieliły już jednoznacznej zgody firmie w przeszłości na zbieranie oraz przetwarzanie numerów telefonu dla tego celu. Numery telefonów osób niebędących użytkownikami mogą być zbierane oraz wykorzystywane tylko dla ściśle ograniczonego celu weryfikacji, czy udzieliły jednoznacznej zgody na przetwarzanie swoich danych, oraz powinny być niezwłocznie później usunięte.

Zestawianie danych osobowych pomiędzy usługami oferowanymi w sieci

Przykład 26: Zestawianie danych osobowych pomiędzy usługami oferowanymi w sieci

Firma internetowa zapewniająca różne usługi w tym wyszukiwarki, dzielenie się nagraniami wideo, sieci społecznościowe, rozwija politykę prywatności, która zawiera klauzulę pozwalającą na „zestawianie wszystkich danych osobowych" zebranych od każdego z użytkowników w odniesieniu do różnych usług, których używają, bez określenia żadnego okresu przechowywania danych. Zgodnie ze stanowiskiem firmy, jest to czynione w celu „zapewnienia możliwie najlepszej jakości usług".

Firma udostępnia pewne narzędzia różnym kategoriom użytkowników, tak aby mogli realizować swoje prawa (tj. dezaktywować ukierunkowaną reklamę, sprzeciwić się ustawieniom określonego typu plików Cookies).

Jednakże dostępne narzędzia nie pozwalają użytkownikom na efektywną kontrolę przetwarzania ich danych: użytkownicy nie mogą kontrolować konkretnych zestawień ich danych pomiędzy usługami oraz użytkownicy nie mogą wyrazić sprzeciwu wobec zestawiania danych ich dotyczących. Ogólnie istnieje nierównowaga pomiędzy prawnie uzasadnionym interesem firmy oraz ochroną podstawowych praw użytkowników i nie powinno się opierać na art. 7 lit. f) jako na podstawie prawnej przetwarzania. Art. 7 lit. a) byłby bardziej odpowiednią podstawą do wykorzystania, zakładając że warunki zgody są spełnione.