GRUPA ROBOCZA ART. 29

844/14/PL
WP 217

Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE

Przyjęta w dniu 9 kwietnia 2014 r.

Spis treści

Streszczenie

W niniejszej opinii przeanalizowano kryteria legalności przetwarzania danych określone w art. 7 dyrektywy 95/46/WE. W opinii tej skupiono się na uzasadnionych interesach administratora danych oraz przedstawiono wytyczne dotyczące sposobu stosowania art. 7 lit. f) w istniejących ramach prawnych oraz zalecenia co do przyszłych ulepszeń.

Artykuł 7 lit. f) jest ostatnią z sześciu podstaw legalnego przetwarzania danych osobowych. Przepis ten nakłada wymóg zachowania równowagi między uzasadnionymi interesami administratora danych lub jakiejkolwiek osoby trzeciej, której dane są ujawniane, a interesami lub prawami podstawowymi osób, których dane dotyczą. Wynik tego testu równowagi pozwoli ustalić, czy art. 7 lit. f) można traktować jako podstawę prawną przetwarzania.

Grupa Robocza Art. 29 uznaje znaczenie i przydatność kryterium określonego w art. 7 lit. f), które w odpowiednich okolicznościach i z zastrzeżeniem odpowiednich gwarancji może być pomocne w zapobieganiu nadmiernemu wykorzystywaniu innych podstawach prawnych. Artykułu 7 lit. f) nie należy traktować jako ostateczności na wypadek rzadkich lub nieoczekiwanych sytuacji, kiedy to uznaje się, że inne podstawy legalnego przetwarzania danych nie mają zastosowania. Nie należy jednak wybierać tego przepisu automatycznie ani nadmiernie rozszerzać jego stosowania w przekonaniu, że jest on mniej ograniczający niż inne podstawy.

Prawidłowa ocena tego, czy art. 7 lit. f) ma zastosowanie, nie jest zwykłym testem równowagi, polegającym tylko na zważeniu dwóch łatwo policzalnych i porównywalnych „wag". W teście tym wymaga się raczej rozważenia w pełni wielu czynników, tak aby zapewnić należyte uwzględnienie interesów i praw podstawowych osób, których dane dotyczą. Jednocześnie test ten jest skalowalny, więc może mieć charakter od prostego po złożony i nie musi być nadmiernie uciążliwy. Czynniki, które należy uwzględnić przy przeprowadzaniu testu równowagi, obejmują:

- charakter i źródło uzasadnionego interesu oraz to, czy przetwarzanie danych jest niezbędne do korzystania z prawa podstawowego, pod innymi względami leży w interesie publicznym lub jest uznawane w danej społeczności;

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

- dodatkowe gwarancje, które mogłyby ograniczyć nadmierny wpływ na osobę, której dane dotyczą, takie jak: minimalizacja danych, technologie służące wzmocnieniu ochrony prywatności; większa przejrzystość, ogólne i bezwarunkowe prawo do rezygnacji oraz możliwość przenoszenia danych.

Grupa Robocza Art. 29 zaleca w przyszłości wprowadzenie do proponowanego rozporządzenia motywu dotyczącego kluczowych czynników, które należy uwzględnić przy stosowaniu testu równowagi. Grupa Robocza Art. 29 zaleca również dodanie motywu zawierającego wymóg, żeby w stosownych przypadkach administrator danych dokumentował swoją ocenę w celu zapewnienia większej rozliczalności. Ponadto Grupa Robocza Art. 29 opowiedziałaby się również za wprowadzeniem przepisu prawa materialnego, zgodnie z którym administrator danych musiałby wyjaśnić osobom, których dane dotyczą, dlaczego jest zdania, że jego interesy nie byłyby podporządkowane

interesom, podstawowym prawom 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 art. 30 ust. 1 lit. a) i ust. 3 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

I. Wprowadzenie

W niniejszej opinii przeanalizowano kryteria legalności przetwarzania danych określone w art. 7 dyrektywy 95/46/WE[1] („dyrektywa"). Skupiono się w szczególności na uzasadnionych interesach administratora danych na mocy art. 7 lit. f).

Kryteria wymienione w art. 7 są związane z szerszą zasadą „legalności" określoną w art. 6 ust. 1 lit. a), który to przepis zawiera wymóg, aby dane osobowe były przetwarzane „rzetelnie i legalnie".

W art. 7 wymaga się, żeby dane osobowe były przetwarzane tylko wówczas, gdy ma zastosowanie co najmniej jedna z sześciu podstaw prawnych wymienionych w tym artykule. W szczególności dane osobowe przetwarza się wyłącznie a) na podstawie jednoznacznej zgody osoby, której dane dotyczą[2]; lub jeśli – krótko mówiąc[3] – przetwarzanie jest konieczne:

b) dla realizacji umowy, której stroną jest osoba, której dane dotyczą;
c) dla wykonania zobowiązania prawnego, któremu administrator danych podlega;
d) dla ochrony żywotnych interesów osób, których dane dotyczą;
e) dla realizacji zadania wykonywanego w interesie publicznym; lub
f) dla potrzeb wynikających z uzasadnionych interesów administratora danych, pod warunkiem przeprowadzenia dodatkowego testu równowagi w odniesieniu do praw i interesów osoby, której dane dotyczą.

Ta ostatnia podstawa zezwala na przetwarzanie danych „konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z[4] podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1". Innymi słowy, w art. 7 lit. f) zezwala się na przetwarzanie pod warunkiem przeprowadzenia testu równowagi, w którym porównuje się

[1] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).
[2] Zob. opinia 15/2011 Grupy Roboczej Art. 29 w sprawie definicji zgody, przyjęta 13.07.2011 r. (WP187).
[3] Przepisy te omówiono bardziej szczegółowo na późniejszym etapie.
[4] Jak wyjaśniono w sekcji III.3.2, angielska wersja dyrektywy wydaje się zawierać literówkę: tekst powinien brzmieć „interests or fundamental rights", a nie „interests for fundamental rights".

uzasadnione interesy administratora danych – lub osoby trzeciej, lub osób, którym dane są ujawniane – z interesami lub prawami podstawowymi osób, których dane dotyczą[5].

Potrzeba przyjęcia bardziej spójnego i zharmonizowanego podejścia w całej Europie

Badania przeprowadzone przez Komisję w ramach przeglądu dyrektywy[6] oraz współpracy i wymiany poglądów między krajowymi organami ochrony danych wykazały brak zharmonizowanej wykładni art. 7 lit. f) dyrektywy, który doprowadził do rozbieżnego jej stosowania w państwach członkowskich. Chociaż w kilku państwach członkowskich istnieje wymóg przeprowadzenia faktycznego testu równowagi, w szczególności art. 7 lit. f) jest czasem błędnie postrzegany jako „otwarta furtka" legitymizująca wszelkie przetwarzanie danych, do którego nie ma zastosowania którakolwiek inna podstawa prawna.

Brak spójnego podejścia może spowodować brak pewności i przewidywalności prawa, może osłabić pozycję osób, których dane dotyczą, a także może nakładać zbędne obciążenie regulacyjne na przedsiębiorstwa i inne organizacje prowadzące działalność transgraniczną. Niespójności te doprowadziły już do sporu przed Trybunałem Sprawiedliwości Unii Europejskiej[7].

Jaśniejsze zrozumienie szóstej podstawy przetwarzania danych (odnoszącej się do „uzasadnionych interesów") i jej związku z innymi podstawami przetwarzania jest zatem szczególnie na czasie, ponieważ wciąż trwają prace nad nowym ogólnym rozporządzeniem o ochronie danych. W szczególności fakt, że zagrożone są prawa podstawowe osób, których dane dotyczą, wiąże się z tym, że stosowanie wszystkich sześciu podstaw powinno odbywać się z uwzględnieniem – w sposób należyty i jednakowy – poszanowania tych praw. Artykuł 7 lit. f) nie powinien stać się łatwym sposobem obejścia przepisów o ochronie danych.

To dlatego Grupa Robocza Art. 29 („Grupa Robocza") w ramach swojego programu prac na lata 2012–2013 zdecydowała się uważnie przeanalizować ten temat oraz – aby wykonać ten program prac[8] – zobowiązała się do opracowania niniejszej opinii.

Wdrożenie istniejących ram prawnych i przygotowanie przyszłych działań

W samym programie prac wyraźnie wskazano dwa cele: „zapewnienie prawidłowego stosowania istniejących ram prawnych" oraz „przygotowanie przyszłych działań".

---

[5] Odesłania do art. 1 ust. 1 nie należy interpretować w sposób ograniczający zakres interesów oraz podstawowych praw i wolności osoby, której dane dotyczą. Odesłanie to służy raczej podkreśleniu ogólnego celu przepisów dotyczących ochrony danych i samej dyrektywy. Artykuł 1 ust. 1 nie odnosi się wyłącznie do ochrony prywatności, ale także do ochrony wszystkich innych „praw i wolności osób fizycznych", przy czym prywatność jest tylko jednym z elementów tych praw i wolności.

[6] W dniu 25 stycznia 2012 r. Komisja Europejska przyjęła pakiet na potrzeby reformy europejskich ram ochrony danych. Pakiet ten obejmuje (i) „komunikat" (COM(2012)9 final), (ii) wniosek dotyczący ogólnego „rozporządzenia o ochronie danych" („proponowane rozporządzenie") (COM(2012)11 final) oraz (iii) wniosek dotyczący „dyrektywy" o ochronie danych w przestrzeni sądowej w zakresie prawa karnego (COM(2012)10 final). Towarzysząca „ocena skutków", która zawiera 10 załączników, została przedstawiona w dokumencie roboczym Komisji (SEC(2012)72 final). Zob. w szczególności badanie pt. „Ocena wdrożenia dyrektywy o ochronie danych", które stanowi załącznik nr 2 do oceny skutków towarzyszącej pakietowi reform Komisji Europejskiej w zakresie ochrony danych.

[7] Zob. s. 7, sekcja II.1 Rys historyczny, *Wdrożenie dyrektywy; wyrok w sprawach ASNEF i FECEMD.*

[8] Zob. program prac na lata 2012–2013 Grupy Roboczej Art. 29 przyjęty dnia 1 lutego 2012 r. (WP190).

Pierwszym celem niniejszej opinii jest zatem zapewnienie wspólnego rozumienia istniejących ram prawnych. Cel ten jest zgodny z wcześniejszymi opiniami na temat innych kluczowych przepisów dyrektywy[9]. Po drugie, w oparciu o analizę w niniejszej opinii sformułowane zostaną również zalecenia dotyczące polityki, które trzeba będzie uwzględnić podczas przeglądu ram prawnych w zakresie ochrony danych.

Struktura opinii

Po krótkim zarysie historii i roli uzasadnionych interesów i innych podstaw przetwarzania danych, który zamieszczono w rozdziale II, w rozdziale III przedstawiona zostanie analiza i wykładnia odpowiednich przepisów dyrektywy z uwzględnieniem wspólnej podstawy w ich wdrożeniu na poziomie krajowym. Analiza ta jest zilustrowana praktycznymi przykładami opartymi na doświadczeniu krajowym. Analiza ta stanowi podstawę zaleceń sformułowanych w rozdziale IV zarówno w odniesieniu do stosowania obecnych ram prawnych, jak i w kontekście przeglądu dyrektywy.

II. Uwagi ogólne i sprawy polityczne

II.1. Rys historyczny

W niniejszym przeglądzie skupiono się na tym, jak rozwinęły się pojęcia legalności i podstawy prawne przetwarzania danych, w tym uzasadnione interesy. Wyjaśniono w szczególności, jak potrzeba istnienia podstawy prawnej została po raz pierwszy zastosowana jako wymóg w kontekście odstępstw od prawa do prywatności, a następnie rozwinęła się w osobny wymóg w kontekście ochrony danych.

Europejska konwencja praw człowieka („EKPC")

Artykuł 8 europejskiej konwencji praw człowieka, którą przyjęto w 1950 r., zawiera prawo do prywatności – czyli poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji każdej osoby. Zakazano w nim ingerencji w prawo do prywatności, z wyjątkiem „przypadków przewidzianych przez ustawę" i „koniecznych w demokratycznym społeczeństwie" w celu zaspokojenia określonych rodzajów wyraźnie wymienionych ważnych interesów publicznych.

W art. 8 EKPC skupiono się na ochronie życia prywatnego i wymaga się uzasadnienia jakiejkolwiek ingerencji w prywatność. Podejście to opiera się na ogólnym zakazie ingerencji w prawo do prywatności i dopuszcza wyjątki jedynie w ściśle określonych warunkach. W przypadkach, w których dochodzi do „ingerencji w prywatność", wymagana jest podstawa prawna, a także określenie celu zgodnego z prawem, co stanowi warunek dokonania oceny konieczności ingerencji. W podejściu tym wyjaśniono, że w EKPC nie przewidziano wykazu możliwych podstaw prawnych, lecz skupiono się na konieczności przedstawienia podstawy prawnej oraz na warunkach, które ta podstawa prawna powinna spełniać.

[9] Na przykład opinia 3/2013 w sprawie celowości, przyjęta 03.04.2013 r. (WP203), opinia 15/2011 w sprawie definicji zgody (przytoczona w 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).

Konwencja nr 108

W konwencji nr 108 Rady Europy[10], otwartej do podpisu w 1981 r., wprowadzono ochronę danych osobowych jako odrębne pojęcie. W owym czasie podstawowym założeniem nie było to, że przetwarzanie danych osobowych należy zawsze postrzegać jako „*ingerencję* w prywatność", ale raczej to, że w celu *chronienia* podstawowych praw i wolności każdej osoby, a zwłaszcza jej prawa do prywatności, przetwarzanie danych osobowych powinno zawsze spełniać określone warunki. W art. 5 ustanowiono więc podstawowe zasady przepisów o ochronie danych, w tym wymóg, że „Dane osobowe będące przedmiotem automatycznego przetwarzania powinny być: a) pozyskiwane oraz przetwarzane rzetelnie i zgodnie z prawem". W konwencji nie podano jednak szczegółowych podstaw przetwarzania[11].

Wytyczne OECD[12]

W wytycznych OECD, które opracowano równolegle z konwencją nr 108 i przyjęto w 1980 r., znajdują się podobne koncepcje „legalności", chociaż pojęcie to jest wyrażone w inny sposób. Wytyczne zostały zaktualizowane w 2013 r., lecz w przypadku zasady legalności nie wprowadzono zmian merytorycznych. Artykuł 7 wytycznych OECD w szczególności stanowi, że „nie powinno być ograniczeń w zakresie gromadzenia danych osobowych i wszelkie takie dane powinny być uzyskiwane w sposób legalny i rzetelny, a w stosownych przypadkach za wiedzą i zgodą osoby, której dane dotyczą". W tym przypadku podstawa prawna, jaką stanowi zgoda, jest wyraźnie wspomniana jako możliwość, którą należy wykorzystywać „w stosownych przypadkach". Będzie to wymagało przeanalizowania przedmiotowych praw i interesów, jak również ocenienia stopnia ingerencji w prywatność związanego z przetwarzaniem. W tym sensie podejście OECD wykazuje pewne podobieństwo do – znacznie bardziej rozwiniętych – kryteriów przewidzianych w dyrektywie 95/46/WE.

Dyrektywa 95/46/WE

Kiedy w 1995 r. przyjęto dyrektywę, była ona oparta na pierwszych instrumentach ochrony danych, w tym konwencji nr 108 i wytycznych OECD. Uwzględniono również wczesne doświadczenia w dziedzinie ochrony danych w niektórych państwach członkowskich.

Oprócz szerszego wymogu określonego w art. 6 ust. 1 lit. a), według którego dane osobowe muszą być przetwarzane „rzetelnie i legalnie", w dyrektywie wprowadzono konkretny zbiór dodatkowych wymagań, które jako takie nie były jeszcze obecne ani w konwencji nr 108, ani w wytycznych OECD: przetwarzanie danych osobowych musi być oparte na jednej z sześciu podstaw prawnych określonych w art. 7.

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

[11] Projekt tekstu zaktualizowanej konwencji, który Komitet Doradczy ds. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (T-PD) przyjął podczas posiedzenia plenarnego w listopadzie 2012 r., stanowi, że przetwarzanie danych może odbywać się na podstawie zgody osoby, której dane dotyczą, lub w oparciu o „pewną uzasadnioną podstawę przewidzianą w przepisach", podobnie jak w Karcie praw podstawowych Unii Europejskiej, którą wspomniano poniżej na s. 9.

[12] Wytyczne OECD w sprawie ochrony prywatności i transgranicznego przepływu danych osobowych, 11 lipca 2013 r.

Wdrożenie dyrektywy; wyrok w sprawach ASNEF i FECEMD[13]

W sprawozdaniu Komisji pt. „Ocena wdrożenia dyrektywy o ochronie danych”[14] podkreślono, że wdrożenie przepisów dyrektywy w prawie krajowym czasami było niezadowalające. W technicznej analizie transpozycji dyrektywy w państwach członkowskich[15] Komisja przedstawiła dalsze szczegóły dotyczące wdrożenia art. 7. W analizie tej wyjaśniono, że podczas gdy w większości państw członkowskich w przepisach określono sześć podstaw prawnych, formułując je w sposób stosunkowo podobny do zastosowanego w dyrektywie, elastyczność tych zasad tak naprawdę doprowadziła do rozbieżnego stosowania przepisów.

Jest to szczególnie istotne w tym kontekście, biorąc pod uwagę fakt, że w wyroku z dnia 24 listopada 2011 r. w sprawach połączonych ASNEF i FECEMD Trybunał Sprawiedliwości orzekł, że Hiszpania nie transponowała poprawnie art. 7 lit. f) dyrektywy, gdyż wprowadziła wymóg, żeby – w przypadku braku zgody osoby, której dane dotyczą – wszelkie istotne wykorzystywane dane były zawarte w powszechnie dostępnych źródłach. W wyroku stwierdzono również, że art. 7 lit. f) ma skutek bezpośredni. Wyrok ten ogranicza zakres swobody uznania, którą państwa członkowskie mają w odniesieniu do wdrożenia art. 7 lit. f). W szczególności nie mogą one przekraczać subtelnej granicy między wyjaśnieniem z jednej strony a ustanowieniem dodatkowych wymagań, które zmieniałyby zakres stosowania art. 7 lit. f), z drugiej strony.

Wyrok ten ma istotne konsekwencje, gdyż wyraźnie dano w nim do zrozumienia, że państwa członkowskie nie mogą wprowadzać w swoich przepisach krajowych dodatkowych jednostronnych ograniczeń i wymogów dotyczących podstaw prawnych legalnego przetwarzania danych. Sądy krajowe oraz inne właściwe organy muszą dokonywać wykładni przepisów krajowych w świetle tego wyroku i w razie potrzeby uchylić wszelkie sprzeczne przepisy i praktyki krajowe.

W świetle tego wyroku tym bardziej istotne jest wypracowanie przez krajowe organy ochrony danych lub europejskich prawodawców jasnego, wspólnego rozumienia w kwestii stosowania art. 7 lit. f). Należy to zrobić w sposób zrównoważony, bez bezpodstawnego ograniczania lub rozszerzania zakresu stosowania tego przepisu.

Karta praw podstawowych

Od momentu wejścia w życie Traktatu z Lizbony w dniu 1 grudnia 2009 r. Karta praw podstawowych Unii Europejskiej („Karta”) ma „taką samą moc prawną jak Traktaty”[16]. W Karcie zapisano ochronę danych osobowych jako prawo podstawowe na mocy art. 8, które jest odrębne od poszanowania życia prywatnego i rodzinnego na mocy art. 7. W art. 8 ustanowiono wymóg istnienia uzasadnionej podstawy przetwarzania. Przepis ten stanowi w szczególności, że dane osobowe muszą być przetwarzane „za zgodą osoby zainteresowanej

[13] Wyrok Trybunału Sprawiedliwości z 24.11.2011 r. w sprawach połączonych C-468/10 i C-469/10 (ASNEF i FECEMD).

[14] Zob. załącznik 2 do oceny skutków towarzyszącej pakietowi reform Komisji w zakresie ochrony danych, przytoczony w przypisie 6 powyżej.

[15] Analiza i badanie wpływu wdrożenia dyrektywy 95/46/WE w państwach członkowskich. Zob. http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf

[16] Zob. art. 6 ust. 1 Traktatu UE.

lub na innej uzasadnionej podstawie przewidzianej ustawą”[17]. Przepisy te wzmacniają zarówno znaczenie zasady legalności, jak i potrzebę odpowiedniej podstawy prawnej przetwarzania danych osobowych.

Proponowane rozporządzenie o ochronie danych

W kontekście procesu przeglądu ochrony danych przedmiotem dyskusji jest obecnie zakres stosowania podstaw legalności na mocy art. 7, a w szczególności zakres stosowania art. 7 lit. f).

W art. 6 proponowanego rozporządzenia wymieniono podstawy zgodnego z prawem przetwarzania danych osobowych. Z pewnymi wyjątkami (które zostaną opisane w dalszej części niniejszego dokumentu) sześć dostępnych podstaw pozostaje w dużej mierze niezmieniona w porównaniu z podstawami, które są obecnie przewidziane w art. 7 dyrektywy. Komisja zaproponowała jednak zapewnienie dalszych wytycznych w formie aktów delegowanych.

Warto zauważyć, że w kontekście pracy w odpowiedniej komisji Parlamentu Europejskiego[18] starano się wyjaśnić pojęcie uzasadnionych interesów w samym proponowanym rozporządzeniu. Opracowano wykaz przypadków, w których uzasadnione interesy administratora danych z reguły byłyby nadrzędne względem uzasadnionych interesów oraz podstawowych praw i wolności osoby, której dane dotyczą, oraz drugi wykaz przypadków, w których ta hierarchia interesów byłaby odwrotna. Wykazy te – ustanowione w przepisach albo w motywach – dostarczają istotnych informacji na potrzeby oceny równowagi pomiędzy prawami i interesami administratora danych a prawami i interesami osoby, której dane dotyczą. Zostały one uwzględnione w niniejszej opinii[19].

II.2. Rola pojęcia

Uzasadnione interesy administratora danych: test równowagi jako ostatnia możliwość?

Artykuł 7 lit. f) wymieniono jako ostatnią z sześciu podstaw umożliwiających legalne przetwarzanie danych osobowych. Przepis ten wymaga przeprowadzenia testu równowagi: to, co jest konieczne dla uzasadnionych interesów administratora danych (lub osób trzecich), trzeba rozważyć w kontekście interesów lub podstawowych praw i wolności osoby, której dane dotyczą. Wynik tego testu równowagi przesądza o tym, czy art. 7 lit. f) można traktować jako podstawę prawną przetwarzania.

Stwarzający możliwość dowolnej interpretacji charakter tego przepisu nasuwa wiele ważnych pytań dotyczących jego dokładnego zakresu i stosowania, co zostanie przeanalizowane w

[17] Zob. art. 8 ust. 2 Karty.

[18] Projekt sprawozdania Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) odnoszącego się do 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)), 16.1.2013 r. („projekt sprawozdania komisji LIBE”). Zob. w szczególności poprawki 101 i 102. Zob. także poprawki przyjęte przez komisję LIBE w dniu 21.10.2013 r. w jej sprawozdaniu końcowym („sprawozdanie końcowe komisji LIBE”).

[19] Zob. sekcja III.3.1, w szczególności wypunktowanie na s. 26–27, gdzie znajduje się niepełny wykaz pewnych najczęstszych sytuacji, w których może pojawić się kwestia uzasadnionego interesu na mocy art. 7 lit. f).

niniejszej opinii. Jak wyjaśniono poniżej, nie oznacza to jednak, że tę możliwość należy postrzegać jako rozwiązanie, z którego można korzystać wyłącznie z umiarem, ostateczność na wypadek rzadkich i nieprzewidzianych sytuacji lub jako ostatnią szansę, w przypadku gdy inne podstawy nie mają zastosowania. Nie należy jej również postrzegać jako preferowanego rozwiązania ani bezpodstawnie rozszerzać jej stosowania, ponieważ podstawa ta byłaby uważana za mniej ograniczającą niż inne podstawy.

Może natomiast okazać się, że art. 7 lit. f) ma swój własny naturalny obszar znaczenia i że może odgrywać bardzo ważną rolę jako podstawa legalnego przetwarzania, pod warunkiem że spełniono szereg kluczowych warunków.

Odpowiednie stosowanie art. 7 lit. f) w odpowiednich okolicznościach i z zastrzeżeniem odpowiednich gwarancji może również pomóc zapobiegać nieprawidłowemu korzystaniu z innych podstaw prawnych lub nadmiernemu poleganiu na tych innych podstawach.

Pierwsze pięć podstaw ustanowionych w art. 7 odnosi się do zgody osoby, której dane dotyczą, ustalenia umownego, zobowiązania prawnego lub innego wyraźnie określonego powodu jako podstawy legalności przetwarzania danych. Jeżeli przetwarzanie opiera się na jednej z tych pięciu podstaw, jest uważane za legalne *a priori*, a zatem jest możliwe tylko z zastrzeżeniem zgodności z innymi mającymi zastosowanie przepisami prawa. Innymi słowy, istnieje założenie, że równowaga pomiędzy różnymi prawami i interesami – w tym administratora danych i osoby, której dane dotyczą – jest zachowana – przyjmując oczywiście, że przestrzegane są wszystkie inne przepisy o ochronie danych. Z drugiej strony w art. 7 lit. f) wymaga się przeprowadzenia *specjalnego* testu w przypadkach, które nie mieszczą się w scenariuszach zdefiniowanych w odniesieniu do podstaw określonych w lit. a)–e). Zapewnia to spełnienie wymogu przeprowadzenia testu równowagi przez każde przetwarzanie, które nie jest uwzględnione w tych scenariuszach, przy należytym uwzględnieniu interesów i praw podstawowych osoby, której dane dotyczą.

Test ten może prowadzić do wniosku, że w niektórych przypadkach szala przechyla się na stronę interesów i praw podstawowych osób, których dane dotyczą, i że w związku z tym działalność związana z przetwarzaniem nie może się odbywać. Z drugiej strony odpowiednia ocena równowagi na mocy art. 7 lit. f), często wraz z możliwością rezygnacji z przetwarzania, w innych przypadkach może być uzasadnioną alternatywą dla niewłaściwego wykorzystania podstawy dotyczącej na przykład „zgody” lub „konieczności realizacji umowy”. Rozpatrywany w ten sposób art. 7 lit. f) stanowi uzupełniającą gwarancję – która wymaga odpowiednich środków – w porównaniu z innymi wcześniej ustalonymi podstawami. Nie powinien zatem być traktowany jako „najsłabsze ogniwo” czy furtka legitymizująca wszelką działalność związaną z przetwarzaniem danych, do której nie ma zastosowania którakolwiek inna podstawa prawna.

Grupa Robocza powtarza, że przy interpretacji zakresu stosowania art. 7 lit. f) dąży do zrównoważonego podejścia, które zapewnia administratorom danych niezbędną elastyczność w sytuacjach, w których nie ma nadmiernego wpływu na osoby, których dane dotyczą, a jednocześnie zapewnia wystarczającą pewność prawa i daje gwarancje osobom, których dane dotyczą, że ten stwarzający możliwość dowolnej interpretacji przepis nie będzie nieprawidłowo stosowany.

II.3. Powiązane pojęcia

Związek art. 7 lit. f) z innymi podstawami legalności

Artykuł 7 zaczyna się od zgody, następnie wyliczone są inne podstawy legalności, w tym umowy i zobowiązania prawne, po czym stopniowo przechodzi się do testu uzasadnionego interesu, która to podstawa jest wymieniona jako ostatnia spośród sześciu dostępnych podstaw. Kolejność, w jakiej wymieniono podstawy prawne na mocy art. 7, była niekiedy interpretowana jako wskazówka co do znaczenia poszczególnych podstaw. Jak już jednak podkreślono w opinii Grupy Roboczej w sprawie definicji zgody[20], w tekście dyrektywy nie ma rozróżnienia prawnego między tymi sześcioma podstawami i nie sugeruje się, że istnieje wśród nich hierarchia. Nic nie wskazuje na to, że art. 7 lit. f) należy stosować tylko w wyjątkowych przypadkach. Z tekstu dyrektywy również w żaden sposób nie wynika, żeby konkretna kolejność sześciu podstaw prawnych miała jakikolwiek skutek istotny z prawnego punktu widzenia. Jednocześnie dokładne znaczenie art. 7 lit. f) i jego związek z innymi podstawami legalności były przez długi czas dość niejasne.

W tym kontekście oraz biorąc pod uwagę różnorodność historyczną i kulturową, a także stwarzający możliwość dowolnej interpretacji język dyrektywy, opracowano różne rodzaje podejścia: niektóre państwa członkowskie skłaniały się ku traktowaniu art. 7 lit. f) jako najmniej preferowanej podstawy, która ma na celu wypełnienie luki tylko w nielicznych wyjątkowych przypadkach, w których żadna z pięciu innych podstaw nie ma lub nie może mieć zastosowania[21]. Inne państwa członkowskie natomiast traktują te podstawę wyłącznie jako jedną z sześciu możliwości, która nie jest ważniejsza ani mniej ważna niż inne możliwości, i która może mieć zastosowanie w wielu różnych sytuacjach, o ile spełnione są niezbędne warunki.

Biorąc pod uwagę te różnice, a także w świetle wyroku w sprawach połączonych ASNEF i FECEMD, ważne jest wyjaśnienie związku podstawy dotyczącej „uzasadnionych interesów" z innymi podstawami legalności – np. w odniesieniu do zgody, umów, zadań wykonywanych w interesie publicznym – a także w odniesieniu do prawa sprzeciwu przysługującego osobie, której dane dotyczą. Może to pomóc lepiej określić rolę i funkcję podstawy dotyczącej uzasadnionych interesów, a tym samym może przyczynić się do pewności prawa.

Należy również zauważyć, że podstawa dotycząca uzasadnionych interesów, wraz z innymi podstawami z wyjątkiem tej dotyczącej zgody, wymaga testu „konieczności". To ściśle ogranicza kontekst, w którym każda z tych podstaw może mieć zastosowanie. Trybunał Sprawiedliwości uznał, że „konieczność" jest autonomicznym pojęciem prawa wspólnotowego[22]. Europejski Trybunał Praw Człowieka także zapewnił pomocne wskazówki[23].

[20] Zob. przypis 2 powyżej.

[21] Należy również zauważyć, że w projekcie sprawozdania komisji LIBE w poprawce 100 zaproponowano oddzielić art. 7 lit. f) od reszty podstaw prawnych, a także zaproponowano dodatkowe wymogi w odniesieniu do korzystania z tej podstawy, w tym większą przejrzystość i rozliczalność. Zostanie to omówione w dalszej części niniejszej opinii.

[22] Wyrok Trybunału Sprawiedliwości z dnia 16 grudnia 2008 r. w sprawie C-524/06 (Heinz Huber przeciwko Bundesrepublik Deutschland), pkt 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.

Ponadto odpowiednia podstawa prawna nie zwalnia administratora danych z jego obowiązków na mocy art. 6 w odniesieniu do rzetelności, legalności, konieczności i proporcjonalności, jak również jakości danych. Na przykład nawet jeśli przetwarzanie danych osobowych opiera się na podstawie dotyczącej uzasadnionych interesów lub realizacji umowy, nie uwzględnia to gromadzenia danych, które są nadmierne w stosunku do określonego celu.

Uzasadnione interesy oraz inne podstawy określone w art. 7 stanowią alternatywy, a zatem wystarczy, jeśli tylko jedna z nich ma zastosowanie. Kumulują się jednak nie tylko z wymogami przewidzianymi w art. 6, lecz także ze wszystkimi innymi zasadami i wymogami ochrony danych, które mogą mieć zastosowanie.

Inne testy równowagi

Artykuł 7 lit. f) nie jest jedynym testem równowagi przewidzianym w dyrektywie. Na przykład art. 9 zawiera wymóg pogodzenia prawa do ochrony danych osobowych z wolnością wypowiedzi. Artykuł ten daje państwom członkowskim możliwość wyłączenia lub odstąpienia w przypadku przetwarzania danych osobowych „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 w wielu innych przepisach dyrektywy wymaga się również analizowania każdego przypadku z osobna, godzenia przedmiotowych interesów i praw oraz przeprowadzania elastycznej oceny wielu czynników. Należą do nich przepisy dotyczące konieczności, proporcjonalności i celowości, wyjątków na mocy art. 13 i badań naukowych, żeby wymienić tylko kilka.

Wydaje się, że dyrektywa rzeczywiście miała pozostawiać pole do interpretacji i godzenia interesów. Oczywiście przynajmniej częściowo miało to służyć zapewnieniu państwom członkowskim większego pola manewru na potrzeby wdrożenia dyrektywy do prawa krajowego. Oprócz tego potrzeba pewnej elastyczności również wynika jednak z samego charakteru prawa do ochrony danych osobowych i prawa do prywatności. Co więcej, te dwa prawa, wraz z większością innych praw podstawowych (ale nie wszystkimi), są uważane za względne, tj. kwalifikowane, prawa człowieka[24]. Te rodzaje praw zawsze muszą być

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 z dnia 25 marca 1983 r. w sprawie Silver i in. przeciwko Zjednoczonemu Królestwu, pkt 97, w którym omówiono wyrażenie „konieczny w społeczeństwie demokratycznym": „przymiotnik »konieczny« nie jest synonimem słowa »niezbędny« ani nie ma elastyczności, którą charakteryzują się takie wyrażenia jak »dopuszczalny«, »zwykły«, »przydatny«, »uzasadniony« lub »pożądany« itp.".

[24] Istnieje tylko kilka praw człowieka, których nie można zestawiać z prawami innych osób ani interesami szerszej społeczności. Są one znane jako prawa bezwzględne. Bez względu na okoliczności prawa te nigdy nie mogą być ograniczone – nawet w stanie wojny lub sytuacji wyjątkowej. Przykładem jest prawo do tego, żeby nie być torturowanym ani traktowanym w sposób nieludzki lub poniżający. Torturowanie lub traktowanie kogoś w sposób nieludzki lub poniżający nigdy nie jest dopuszczalne, niezależnie od okoliczności. Przykłady nieabsolutnych praw człowieka obejmują prawo do poszanowania życia prywatnego i rodzinnego, prawo do wolności wypowiedzi oraz prawo do wolności myśli, sumienia i religii.

interpretowane w kontekście. Prawa te można zestawiać z prawami innych osób, o ile istnieją odpowiednie gwarancje. W niektórych sytuacjach – a także z zastrzeżeniem odpowiednich gwarancji – prawa te mogą być również ograniczone ze względów interesu publicznego.

II.4. Kontekst i skutki strategiczne

Zapewnianie legalności, ale także elastyczności: środki określania wymogów na mocy art. 7 lit. f)

Obecny tekst art. 7 lit. f) dyrektywy stwarza możliwość dowolnej interpretacji. Oznacza to, że można się na nim opierać w wielu różnych sytuacjach, o ile spełnione są jego wymogi, w tym w zakresie testu równowagi. Taka elastyczność może jednak mieć także negatywne konsekwencje Ważną rolę odgrywałyby dalsze wytyczne, które mogłyby zapobiec wynikającemu z tej elastyczności niespójnemu stosowaniu przepisów na szczeblu krajowym lub brakowi pewności prawa.

W proponowanym rozporządzeniu Komisja przewiduje takie wytyczne w formie aktów delegowanych. Inne warianty obejmują zapewnienie wyjaśnień i szczegółowych przepisów w tekście samego proponowanego rozporządzenia[25] lub powierzenie Europejskiej Radzie Ochrony Danych („EROD") zadania dostarczenia dodatkowych wytycznych w tym zakresie.

Każdy z tych wariantów ma zalety i wady. Gdyby ocena miała być przeprowadzana dla każdego przypadku z osobna bez dalszych wytycznych, stwarzałoby to ryzyko niespójnego stosowania i braku przewidywalności, do czego dochodziło w przeszłości.

Z drugiej strony zapewnienie w tekście samego proponowanego rozporządzenia szczegółowych i wyczerpujących wykazów sytuacji, w których uzasadnione interesy administratora danych z zasady przeważają nad prawami podstawowymi osoby, której dane dotyczą, lub odwrotnie, może stwarzać ryzyko wprowadzania w błąd przez te wykazy lub nadania im zbyt nakazowego charakteru, lub powodować oba te rodzaje ryzyka.

Niemniej jednak podejście to mogłoby zainspirować do opracowania wyważonego rozwiązania – zawarcia w samym proponowanym rozporządzeniu pewnych bardziej szczegółowych przepisów i zapewnienia dalszych wytycznych w aktach delegowanych lub w wytycznych Europejskiej Rady Ochrony Danych[26].

Analiza zawarta w rozdziale III ma na celu stworzenie podstaw do znalezienia takiego podejścia, które nie będzie ani zbyt ogólne, a przez to bez znaczenia, ani zbyt szczegółowe, a wskutek tego nadmiernie sztywne.

[25] Zob. sekcja II.1 Rys historyczny, *Proponowane rozporządzenie o ochronie danych,* s. 10.

[26] Jeżeli chodzi o akty delegowane i wytyczne Europejskiej Rady Ochrony Danych, w opinii 8/2012 Grupy Roboczej przedstawiającej dalsze uwagi dotyczące dyskusji na temat reformy ochrony danych, przyjętej 05.10.2012 r. (WP199), zdecydowanie opowiedziano się za tymi drugimi (zob. pkt 13–14).

III. Analiza przepisów

III.1. Przegląd art. 7

W art. 7 wymaga się, żeby dane osobowe były przetwarzane tylko wówczas, gdy ma zastosowanie co najmniej jedna z sześciu podstaw prawnych wymienionych w tym artykule. Przed przeanalizowaniem każdej z tych podstaw w sekcji III.1 przedstawiono przegląd art. 7 i jego związek z art. 8 dotyczącym szczególnych kategorii danych.

III.1.1. Zgoda lub „konieczne dla..."

Można dokonać rozróżnienia między przypadkiem, w którym dane osobowe są przetwarzane na podstawie jednoznacznej zgody osoby, której dane dotyczą (art. 7 lit. a)), a pozostałymi pięcioma przypadkami (art. 7 lit. b)–f)). Krótko mówiąc, te pięć przypadków opisuje scenariusze, w których przetwarzanie może być konieczne w określonym kontekście, np. realizacji umowy, której stroną jest osoba, której dane dotyczą, wykonania zobowiązania prawnego, któremu administrator danych podlega itp.

W pierwszym przypadku na mocy art. 7 lit. a) to same osoby, których dane dotyczą, zezwalają na przetwarzanie ich danych osobowych. To do nich należy decyzja, czy zezwolić na przetwarzanie ich danych. Jednocześnie zgoda nie eliminuje potrzeby poszanowania zasad przewidzianych w art. 6[27]. Ponadto zgoda musi jeszcze spełniać pewne podstawowe warunki, aby była legalna, jak wyjaśniono w opinii 15/2011 Grupy Roboczej[28]. Ponieważ przetwarzanie danych użytkownika ostatecznie zależy od jego uznania, nacisk kładzie się na ważność i zakres zgody osoby, której dane dotyczą.

Innymi słowy, pierwsza podstawa, art. 7 lit. a), dotyczy przede wszystkim samostanowienia osoby, której dane dotyczą, jako podstawy legalności. Wszystkie inne podstawy natomiast umożliwiają przetwarzanie – z zastrzeżeniem gwarancji i środków – w sytuacjach, w których przetwarzanie danych w określonym kontekście w celu zrealizowania określonego uzasadnionego interesu jest – niezależnie od zgody – właściwe i konieczne.

W lit. b), c), d) i e) określono poszczególne kryteria legalności przetwarzania:

b) dla realizacji umowy, której stroną jest osoba, której dane dotyczą;
c) dla wykonania zobowiązania prawnego, któremu administrator danych podlega;
d) dla ochrony żywotnych interesów osób, których dane dotyczą;
e) realizacja zadania wykonywanego w interesie publicznym.

Przepis zawarty w lit. f) jest mniej szczegółowy i dotyczy, w ujęciu bardziej ogólnym, (wszelkiego rodzaju) uzasadnionego interesu administratora danych (w dowolnym

[27] Wyrok niderlandzkiego Sądu Najwyższego z dnia 9 września 2011 r. w sprawie ECLI:NL:HR:2011:BQ8097, pkt 3.3 lit. e), w kwestii zasady proporcjonalności. Zob. także s. 7 opinii 15/2011 Grupy Roboczej przywołanej w przypisie 2 powyżej: „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] Zob. s. 11–25 opinii 15/2011, przywołanej w przypisie 2 powyżej.

kontekście). Ten ogólny przepis jest jednak wyraźnie związany z wymogiem przeprowadzenia dodatkowego testu równowagi, którego celem jest ochrona interesów i praw osób, których dane dotyczą, jak zostanie wykazane poniżej w sekcji III.2.

Ocena tego, czy kryteria określone w art. 7 lit. a)–f) zostały spełnione, jest w każdym przypadku wstępnie przeprowadzana przez administratora danych zgodnie z prawem właściwym oraz z wytycznymi dotyczącymi stosowania tego prawa. W drugim przypadku legalność przetwarzania może być przedmiotem dalszej oceny i może ewentualnie zostać zakwestionowana przez osoby, których dane dotyczą, inne zainteresowane strony, organy ochrony danych, a ostatecznie kwestię legalności rozstrzygają sądy.

Aby zakończyć ten krótki przegląd, należy zauważyć, że, jak zostanie to omówione w sekcji III.3.6, przynajmniej w przypadkach, o których mowa w lit. e) i f), osoba, której dane dotyczą, może skorzystać z prawa sprzeciwu przewidzianego w art. 14[29]. Doprowadzi to do nowej oceny przedmiotowych interesów, lub, w przypadku marketingu bezpośredniego (art. 14 lit. b)), sprawi, że administrator danych będzie musiał zaprzestać przetwarzania danych osobowych bez dalszej oceny.

III.1.2. Związek z art. 8

W art. 8 dyrektywy dokładniej reguluje się przetwarzanie pewnych szczególnych kategorii danych osobowych. Dotyczy to w szczególności 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" (art. 8 ust. 1) oraz danych „dotyczących przestępstw, wyroków skazujących" (art. 8 ust. 5).

Przetwarzanie takich danych jest w zasadzie zabronione, z zastrzeżeniem pewnych wyjątków. W art. 8 ust. 2 lit. a)–e) przewidziano szereg wyjątków od tego zakazu. W art. 8 ust. 3 i 4 przewidziano dalsze wyjątki. Niektóre z tych przepisów są podobne do przepisów określonych w art. 7 lit. a)–f), lecz nie są identyczne.

Szczególne warunki zawarte w art. 8, jak również fakt, że niektóre z podstaw wymienionych w art. 7 przypominają warunki określone w art. 8, sprawiają, że pojawia się kwestia związku między tymi dwoma przepisami.

Jeżeli art. 8 ma stanowić *lex specialis*, należy rozważyć, czy całkowicie wyklucza możliwość stosowania art. 7. Jeśli tak, oznaczałoby to, że szczególne kategorie danych osobowych można przetwarzać bez konieczności spełnienia wymogów art. 7, pod warunkiem że stosuje się jeden z wyjątków przewidzianych w art. 8. Jest jednak również możliwe, że związek między tymi przepisami jest bardziej złożony i że art. 7 i 8 powinny być stosowane łącznie[30].

[29] W nawiązaniu do art. 14 lit. a) prawo to stosuje się „z zastrzeżeniem odmiennych postanowień ustawodawstwa krajowego". Na przykład w Szwecji w prawie krajowym nie przewidziano możliwości wniesienia sprzeciwu wobec przetwarzania odbywającego się na podstawie art. 7 lit. e).

[30] Ponieważ art. 8 jest ustanowiony jako *zakaz z wyjątkami*, wyjątki te mogą być postrzegane jako wymogi, które tylko ograniczają zakres zakazu, ale same w sobie nie stanowią wystarczającej podstawy prawnej przetwarzania. Zgodnie z tą interpretacją stosowanie wyjątków przewidzianych w art. 8 nie wyklucza stosowania wymogów określonych w art. 7, a w stosownych przypadkach oba te przepisy muszą być stosowane łącznie.

Tak czy owak, jasne jest, że celem polityki jest zapewnienie dodatkowej ochrony szczególnym kategoriom danych. Dlatego ostateczny wynik tej analizy powinien być równie jasny: stosowanie art. 8, czy samodzielnie, czy w połączeniu z art. 7, ma na celu zapewnienie wyższego poziomu ochrony szczególnym kategoriom danych.

W praktyce, podczas gdy w niektórych przypadkach w art. 8 przewidziane są bardziej rygorystyczne wymogi – takie jak „wyraźna" zgoda, o której mowa w art. 8 ust. 2 lit. a), w porównaniu z „jednoznacznym wyrażeniem zgody", o którym mowa w art. 7 – nie odnosi się to do wszystkich przepisów. Pewne wyjątki przewidziane w art. 8 nie wydają się równoważne podstawom wymienionym w art. 7 ani nie wydają się bardziej rygorystyczne niż te podstawy. Niewłaściwe byłoby na przykład stwierdzenie, że fakt, iż ktoś wyraźnie upublicznił specjalne kategorie danych na mocy art. 8 ust. 2 lit. e), będzie – zawsze i samo w sobie – warunkiem wystarczającym do umożliwienia wszelkiego rodzaju przetwarzania danych, bez oceny równowagi przedmiotowych praw i interesów, czego wymaga się w art. 7 lit. f)[31].

W niektórych sytuacjach fakt, że administrator danych jest partią polityczną, również mógłby skutkować zniesieniem zakazu przetwarzania szczególnych kategorii danych na mocy art. 8 ust. 2 lit. d). To jednak nie oznacza, że jakiekolwiek przetwarzanie wchodzące w zakres stosowania tego przepisu jest siłą rzeczy legalne. Tę kwestię trzeba ocenić oddzielnie, a administrator danych może mieć obowiązek wykazania, że na przykład przetwarzanie danych jest konieczne dla realizacji umowy (art. 7 lit. b)), lub że jego uzasadniony interes na mocy art. 7 lit. f) jest nadrzędny. W tym ostatnim przypadku po ocenieniu, że administrator danych spełnia wymogi art. 8, trzeba przeprowadzić test równowagi na mocy art. 7 lit. f).

Podobnie sam fakt, że „przetwarzanie danych wymagane jest do celów medycyny prewencyjnej, diagnostyki medycznej, świadczenia opieki lub leczenia, lub też zarządzania opieką zdrowotną" oraz to, że przetwarzanie tych danych podlega obowiązkowi zachowania tajemnicy zawodowej – co wszystko wspomniano w art. 8 ust. 3 – oznacza, że takie przetwarzanie danych szczególnie chronionych jest *wyłączone z zakazu* ustanowionego w art. 8 ust. 1. To jednak niekoniecznie wystarcza, żeby zapewnić również legalność na mocy art. 7, i będzie wymagało podstawy prawnej, takiej jak: umowa z pacjentem na mocy art. 7 lit. b), zobowiązanie prawne na mocy art. 7 lit. c), realizacja zadania wykonywanego w interesie publicznym na mocy art. 7 lit. e) lub ocena na mocy art. 7 lit. f).

Podsumowując, Grupa Robocza uważa, że analizę trzeba przeprowadzać w każdym przypadku indywidualnie, bez względu na to, czy w samym art. 8 przewidziano bardziej rygorystyczne, wystarczające warunki[32], czy łączne zastosowanie zarówno art. 8, jak i art. 7 jest wymagane do zapewnienia pełnej ochrony osób, których dane dotyczą. W żadnym

[31] Ponadto art. 8 ust. 2 lit. e) nie należy interpretować *a contrario* jako oznaczającego, że w przypadku gdy dane podawane do wiadomości publicznej przez osobę, której dane dotyczą, nie są szczególnie chronione, mogą być przetwarzane bez żadnych dodatkowych warunków. Publicznie dostępne dane są nadal danymi osobowymi objętymi wymogami ochrony danych, w tym wymogiem zgodności z art. 7, niezależnie od tego, czy są to dane szczególnie chronione.

[32] Zob. analiza przeprowadzona w opinii Grupy Roboczej dotyczącej WADA, pkt 3.3, w której uwzględniono zarówno art. 7, jak i art. 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).

przypadku wynik badania nie może prowadzić do niższego poziomu ochrony szczególnych kategorii danych[33].

Oznacza to również, że administrator danych przetwarzający szczególne kategorie danych nigdy nie może powoływać się *wyłącznie* na podstawę prawną na mocy art. 7, aby uzasadnić działalność związaną z przetwarzaniem danych. W stosownych przypadkach art. 7 nie będzie *nadrzędny*, ale zawsze będzie stosował się w sposób *łączny* z art. 8, aby zapewnić przestrzeganie wszystkich odpowiednich gwarancji i środków. Będzie to tym bardziej istotne, w przypadku gdy państwa członkowskie zdecydują się dodać dodatkowe wyłączenia – jak przewidziano w art. 8 ust. 4 – do tych, które określono w art. 8.

III.2. Artykuł 7 lit. a)–e)

Sekcja III.2 zawiera krótki przegląd każdej z podstaw prawnych określonych w art. 7 lit. a)–e) dyrektywy, po czym w sekcji III.3 niniejszej opinii skupiono się na art. 7 lit. f). W analizie tej zostaną również podkreślone niektóre najczęstsze wspólne płaszczyzny między tymi podstawami prawnymi, na przykład odnoszące się do „umowy", „zobowiązania prawnego" i „uzasadnionego interesu", w zależności od konkretnego kontekstu i okoliczności danego przypadku.

III.2.1. Zgoda

Zgodę jako podstawę prawną przeanalizowano w opinii 15/2011 Grupy Roboczej w sprawie definicji zgody. Z głównych wniosków zawartych w tej opinii wynika, że zgoda jest jedną z kilku podstaw prawnych przetwarzania danych osobowych, a nie podstawą główną. Ma ważną rolę, ale to nie wyklucza możliwości, w zależności od kontekstu, że inne podstawy prawne mogą być bardziej odpowiednie z punktu widzenia administratora danych albo osoby, której dane dotyczą. Zgoda, jeśli jest prawidłowo wykorzystywana, jest narzędziem dającym osobie, której dane dotyczą, kontrolę nad przetwarzaniem tych danych. Jeśli jest stosowana niewłaściwie, kontrola ze strony osoby, której dane dotyczą, staje się iluzoryczna, a zgoda stanowi nieodpowiednią podstawę przetwarzania.

Wśród swoich zaleceń Grupa Robocza podkreśliła konieczność 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]. Grupa Robocza stwierdziła również, że administratorzy danych powinni mieć obowiązek wprowadzenia mechanizmów wykazujących uzyskanie zgody (w kontekście ogólnego obowiązku rozliczalności) i poprosiła prawodawcę o dodanie wyraźnego wymogu dotyczącego jakości i dostępności informacji stanowiących podstawę zgody.

[33] Jest rzeczą oczywistą, że również w przypadku stosowania art. 8 trzeba zapewnić poszanowanie innych przepisów dyrektywy, w tym art. 6.
[34] Zob. s. 36 opinii 15/2011 Grupy Roboczej w sprawie definicji zgody.

III.2.2. Umowa

Artykuł 7 lit. b) stanowi podstawę prawną w sytuacjach, w których „przetwarzanie danych 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 dwa różne scenariusze.

i) Po pierwsze przepis ten obejmuje sytuacje, w których przetwarzanie jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą. Może to obejmować na przykład przetwarzanie adresu osoby, której dane dotyczą, żeby można było dostarczyć towary zakupione przez nią w Internecie, lub przetwarzanie danych karty kredytowej w celu dokonania płatności. W kontekście zatrudnienia podstawa ta może przykładowo umożliwiać przetwarzanie informacji o wynagrodzeniu i danych rachunku bankowego, żeby można było wypłacić wynagrodzenie.

   Przepis ten trzeba interpretować w sposób zawężający. Nie obejmuje on sytuacji, w których przetwarzanie nie jest rzeczywiście *konieczne* dla realizacji umowy, ale raczej jednostronnie narzucone osobie, której dane dotyczą, przez administratora danych. Również fakt, że niektóre czynności przetwarzania danych są objęte umową, nie oznacza automatycznie, że przetwarzanie to jest niezbędne do jej realizacji. Na przykład art. 7 lit. b) nie jest odpowiednią podstawą prawną w odniesieniu do tworzenia profilu dotyczącego upodobań i stylu życia użytkownika w oparciu o jego kliknięcia na stronie internetowej i zakupione przedmioty. Wynika to z tego, że administratorowi danych nie zlecono tworzenia profili, a raczej na przykład dostarczanie określonych towarów i usług. Nawet jeśli ta działalność związana z przetwarzaniem jest wyraźnie wymieniona drobnym drukiem w umowie, sam ten fakt nie czyni jej „niezbędną" dla realizacji umowy.

   Istnieje tu wyraźny związek pomiędzy oceną konieczności a zgodnością z zasadą celowości. Istotne jest określenie dokładnego *powodu* umowy, czyli jej istoty i podstawowego celu, ponieważ to względem nich będzie badane, czy przetwarzanie danych jest konieczne dla realizacji tej umowy.

   W pewnych sytuacjach budzących wątpliwości określenie, czy przetwarzanie danych jest konieczne dla realizacji umowy, może być dyskusyjne lub może wymagać ustalenia bardziej szczegółowych informacji. Na przykład utworzenie wewnętrznej bazy danych kontaktowych pracowników przedsiębiorstwa, zawierającej imię i nazwisko, adres służbowy, numer telefonu i adres e-mail wszystkich pracowników i mającej na celu umożliwienie pracownikom kontaktowania się ze współpracownikami, może w pewnych sytuacjach być uznane za niezbędne dla realizacji umowy na mocy art. 7 lit. b), ale może być również legalne na mocy art. 7 lit. f), jeżeli wykazano nadrzędny interes administratora danych i zastosowano wszystkie odpowiednie środki, w tym na przykład przeprowadzono stosowne konsultacje z przedstawicielami pracowników.

   Inne przypadki, na przykład elektroniczne monitorowanie korzystania przez pracowników z Internetu, poczty elektronicznej lub telefonu bądź nadzór wideo nad pracownikami, są bardziej oczywistym przykładem przetwarzania, które może wykraczać poza to, co jest konieczne dla realizacji umowy o pracę, choć może to także zależeć od charakteru zatrudnienia. Zapobieganie oszustwom – co może

obejmować między innymi monitorowanie i profilowanie klientów – to kolejny typowy obszar, który może być uznany za wykraczający poza to, co jest niezbędne dla realizacji umowy. Takie przetwarzanie mogłoby wówczas być legalne na innej podstawie określonej w art. 7, na przykład odbywać się w stosownych przypadkach na podstawie zgody, zobowiązania prawnego lub uzasadnionego interesu administratora danych (art. 7 lit. a), c) lub f))[35]. W tym ostatnim przypadku przetwarzanie powinno być objęte dodatkowymi gwarancjami i środkami w celu odpowiedniego chronienia interesów lub praw i wolności osób, których dane dotyczą.

Artykuł 7 lit. b) stosuje się tylko do tego, co jest konieczne dla *realizacji* umowy. Nie ma zastosowania do wszystkich dalszych działań wywołanych niezgodnością ani do innych incydentów zaistniałych podczas wykonywania umowy. Jeśli tylko przetwarzanie obejmuje normalne wykonanie umowy, może wchodzić w zakres stosowania art. 7 lit. b). Jeśli w ramach realizacji umowy wystąpi incydent, który wywołuje konflikt, przetwarzanie danych może przybrać inny obrót. Przetwarzanie podstawowych informacji na temat osoby, której dane dotyczą, takich jak: imię i nazwisko, adres i odniesienie do niewykonanych zobowiązań umownych, w celu wysłania formalnych przypomnień powinno nadal być traktowane jako działanie wchodzące w zakres przetwarzania danych koniecznego dla realizacji umowy. W odniesieniu do bardziej skomplikowanego przetwarzania danych, które może odbywać się przy udziale osób trzecich, na przykład zewnętrznej windykacji należności lub pozwania do sądu klienta, który nie zapłacił za usługę, można by argumentować, że takie przetwarzanie nie odbywa się już w ramach „normalnego" wykonywania umowy, a zatem nie wchodzi w zakres stosowania art. 7 lit. b). Nie powodowałoby to jednak, że takie przetwarzanie byłoby nielegalne – administrator danych ma uzasadniony interes w poszukiwaniu środków prawnych zapewniających poszanowanie jego praw wynikających z umowy. Można przywoływać inne podstawy prawne, takie jak art. 7 lit. f), z zastrzeżeniem odpowiednich gwarancji i środków oraz pozytywnego wyniku testu równowagi[36].

ii) Po drugie, art. 7 lit. b) obejmuje także przetwarzanie, które ma miejsce *przed* zawarciem umowy. Dotyczy to stosunków przedumownych, pod warunkiem że kroki podejmowane są na wniosek osoby, której dane dotyczą, a nie z inicjatywy administratora danych lub osoby trzeciej. Na przykład jeśli dana osoba życzy sobie, żeby detalista przesłał jej ofertę produktu, przetwarzanie w tych celach, takie jak przechowywanie danych adresowych i informacji o tym, czego zażądano, przez ograniczony okres, będzie właściwe na tej podstawie prawnej. Podobnie jeśli dana osoba poprosi ubezpieczyciela o przedstawienie oferty dotyczącej jej samochodu, ubezpieczyciel może przetwarzać konieczne dane, na przykład markę i wiek pojazdu oraz inne istotne i proporcjonalne dane, w celu przygotowania oferty.

[35] Inny przykład, w którym zastosowanie ma wiele podstaw prawnych, można znaleźć w opinii 15/2011 Grupy Roboczej w sprawie definicji zgody (przywołanej w przypisie 2). W przypadku kupna samochodu administrator danych może być uprawniony do przetwarzania danych osobowych w różnych celach i na różnych podstawach:
- danych niezbędnych w celu kupna samochodu – art. 7 lit. b);
- w celu przetwarzania dokumentów samochodu: art. 7 lit. c);
- w celu zarządzania klientami (np. aby zapewnić serwisowanie samochodu przez powiązane przedsiębiorstwa w UE): art. 7 lit. f);
- w celu przekazania danych osobom trzecim dla ich własnych działań marketingowych: art. 7 lit. a).

[36] W odniesieniu do szczególnych kategorii danych może zajść potrzeba uwzględnienia również art. 8 ust. 1 lit. e) – „konieczne do ustalenia, wykonania lub ochrony roszczeń prawnych".

Jednak szczegółowe podstawowe kontrole, na przykład przetwarzanie danych pochodzących z badań lekarskich, zanim zakład ubezpieczeń zapewni wnioskodawcy ubezpieczenie zdrowotne lub ubezpieczenie na życie, nie byłoby uznane za niezbędne działania podjęte na wniosek osoby, której dane dotyczą. Kontrole informacji kredytowych przed udzieleniem kredytu również nie są wykonywane na *wniosek* osoby, której dane dotyczą, na mocy art. 7 lit. b), a raczej na mocy art. 7 lit. f) lub zgodnie ze zobowiązaniem prawnym banków do sprawdzenia danych w oficjalnym rejestrze dłużników, tj. na mocy art. 7 lit. c).

Marketing bezpośredni z inicjatywy detalisty/administratora danych również nie będzie możliwy na tej podstawie. W niektórych przypadkach art. 7 lit. f) mógłby stanowić odpowiednią podstawę prawną zamiast art. 7 lit. b), z zastrzeżeniem odpowiednich gwarancji i środków oraz pozytywnego wyniku testu równowagi. W innych przypadkach, w tym tych związanych z rozległym profilowaniem, udostępnianiem danych, internetowym marketingiem bezpośrednim lub reklamą behawioralną, należy wziąć pod uwagę zgodę na mocy art. 7 lit. a), jak wynika z poniższej analizy[37].

III.2.3. Zobowiązanie prawne

Artykuł 7 lit. c) stanowi podstawę prawną w sytuacjach, w których „przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega". Może to mieć miejsce na przykład w przypadku, gdy pracodawca musi zgłaszać dane dotyczące wynagrodzeń swoich pracowników do organów ubezpieczenia społecznego lub podatkowych lub gdy instytucje finansowe są zobowiązane do zgłaszania właściwym organom pewnych podejrzanych transakcji na mocy przepisów dotyczących przeciwdziałania praniu pieniędzy. Może to również być zobowiązanie, któremu podlega organ publiczny, ponieważ nic nie ogranicza stosowania art. 7 lit. c) do sektora prywatnego lub publicznego. Dotyczyłoby to na przykład gromadzenia danych przez organ lokalny na potrzeby wymierzania kar za parkowanie w miejscu niedozwolonym.

Artykuł 7 lit. c) wykazuje podobieństwa do art. 7 lit. e), gdyż zadanie leżące w interesie publicznym często jest oparte na przepisie prawnym lub wywodzi się z niego. Zakres stosowania art. 7 lit. c) jest jednak ściśle określony.

Aby art. 7 lit. c) miał zastosowanie, zobowiązanie musi być nałożone przez przepisy (a nie na przykład przez ustalenia umowne). Przepisy te muszą spełniać wszystkie odpowiednie warunki, aby zobowiązanie było ważne i wiążące, a także muszą być zgodne z przepisami o ochronie danych, w tym z wymogiem konieczności, proporcjonalności[38] i celowości.

Trzeba również podkreślić, że art. 7 lit. c) odnosi się do przepisów Unii Europejskiej lub państwa członkowskiego. Zobowiązania wynikające z przepisów państw trzecich (jak na przykład obowiązek utworzenia systemów informowania o nieprawidłowościach na mocy ustawy Sarbanesa-Oxleya z 2002 r. w Stanach Zjednoczonych), nie są objęte tą podstawą.

[37] Zob. sekcja III.3.6 lit. b), „Przykład: ewolucja podejścia do marketingu bezpośredniego", s. 51–52.
[38] Zob. również opinia 01/2014 Grupy Roboczej w sprawie stosowania pojęć konieczności i proporcjonalności oraz ochrony danych w sektorze egzekwowania prawa, przyjęta 27.02.2014 r. (WP 211).

Aby zobowiązanie prawne państwa trzeciego było ważne, musiałoby zostać oficjalnie uznane i włączone do porządku prawnego danego państwa członkowskiego, na przykład na mocy umowy międzynarodowej[39]. Z drugiej strony, konieczność dotrzymania zobowiązania zagranicznego może stanowić uzasadniony interes administratora danych, ale jedynie z zastrzeżeniem testu równowagi zgodnie z art. 7 lit. f) oraz pod warunkiem że zapewnione są odpowiednie gwarancje, takie jak te zatwierdzone przez właściwy organ ochrony danych.

Administrator danych nie może mieć wyboru, czy ma wywiązać się z zobowiązania. Dobrowolne zobowiązania jednostronne i partnerstwa publiczno-prywatne, w ramach których przetwarzanie danych wychodzi poza to, co jest wymagane przez prawo, nie są zatem objęte art. 7 lit. c). Na przykład jeżeli – bez jasnego i konkretnego zobowiązania prawnego, aby to zrobić – dostawca usług internetowych decyduje się monitorować użytkowników swoich usług w celu zwalczania nielegalnego pobierania treści, art. 7 lit. c) nie będzie odpowiednią podstawa prawną do tego celu.

Ponadto samo zobowiązanie prawne musi być wystarczająco jasne co do wymaganego na jego mocy przetwarzania danych osobowych. Artykuł 7 lit. c) stosuje się zatem na podstawie przepisów prawnych odnoszących się bezpośrednio do charakteru i przedmiotu przetwarzania. Administrator danych nie powinien mieć nadmiernego zakresu swobody uznania co do sposobu wywiązania się ze zobowiązania prawnego.

W niektórych przypadkach w prawodawstwie może być ustanowiony tylko cel ogólny, a bardziej szczegółowe zobowiązania mogą być nałożone na innym poziomie, na przykład w prawie wtórnym lub w wiążącej decyzji organu publicznego w konkretnej sprawie. Może to również prowadzić do zobowiązań prawnych na mocy art. 7 lit. c), pod warunkiem że charakter i przedmiot przetwarzania jest prawidłowo określony i istnieje odpowiednia podstawa prawna.

Sytuacja jest jednak inna, jeżeli organ regulacyjny określa tylko ogólne wytyczne dotyczące polityki i warunki, w których mógłby rozważyć użycie swoich uprawnień wykonawczych (np. wytyczne regulacyjne dla instytucji finansowych w sprawie pewnych norm w zakresie należytej staranności). W takich przypadkach działalność związaną z przetwarzaniem należy poddać ocenie na mocy art. 7 lit. f) i uznać za legalną wyłącznie pod warunkiem przeprowadzenia dodatkowego testu równowagi[40].

Ogólnie rzecz biorąc, należy zauważyć, że może wydawać się, iż niektóre rodzaje działalności związanej z przetwarzaniem niemal wchodzą w zakres stosowania art. 7 lit. c) lub b), lecz nie w pełni spełniają kryteria zastosowania tych podstaw. To nie znaczy koniecznie, że takie przetwarzanie jest zawsze nielegalne: czasami może być legalne, lecz na mocy art. 7 lit. f), z zastrzeżeniem dodatkowego testu równowagi.

---

[39] Zob. w tej kwestii sekcja 4.2.2 opinii 10/2006 Grupy Roboczej w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Worldwide Interbank Financial Telecommunication, SWIFT), przyjęta 20.11.2006 r. (WP128), oraz opinia 1/2006 Grupy Roboczej 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 rolę w ocenie uzasadnionego interesu administratora danych (zob. sekcja III.3.4 lit. a), w szczególności s. 36).

III.2.4. Żywotny interes

Artykuł 7 lit. d) stanowi podstawę prawną w sytuacjach, w których „przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osób, których dane dotyczą". Sformułowanie to różni się od języka zastosowanego w art. 8 ust. 2 lit. c), który jest bardziej szczegółowy i odnosi się do sytuacji, gdy „przetwarzanie danych 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".

Oba przepisy wydają się jednak sugerować, że ta podstawa prawna powinna mieć ograniczone zastosowanie. Po pierwsze, wyrażenie „żywotny interes" wydaje się ograniczać stosowanie tej podstawy do kwestii życia i śmierci lub co najmniej zagrożeń, które stwarzają ryzyko urazu lub innej szkody dla zdrowia osoby, której dane dotyczą (lub w przypadku art. 8 ust. 2 lit. c) również innej osoby).

W motywie 31 potwierdzono, że celem tej podstawy prawnej jest zapewnienie „ochrony interesu, który jest niezbędny dla życia osoby, której dane dotyczą". W dyrektywie nie określono jednak dokładnie, czy zagrożenie musi być bezpośrednie. To rodzi problemy dotyczące zakresu gromadzenia danych, na przykład w charakterze środka zapobiegawczego lub na szeroką skalę, jak gromadzenie danych pasażerów linii lotniczych, w przypadku gdy stwierdzono ryzyko wybuchu epidemii lub zdarzenie naruszające ochronę.

Grupa Robocza uważa, że wykładnia tego przepisu musi być zawężająca, zgodnie z duchem art. 8. Mimo że art. 7 lit. d) nie ogranicza korzystania z tej podstawy konkretnie do sytuacji, w których zgody nie można zastosować jako podstawy prawnej z przyczyn określonych w art. 8 ust. 2 lit. c), uzasadnione jest założenie, że w sytuacjach, w których istnieje możliwość i potrzeba zażądania wyrażenia ważnej zgody, należy rzeczywiście dążyć do uzyskania tej zgody, kiedy tylko jest to możliwe. Ograniczałoby to także stosowanie tego przepisu do analizy poszczególnych przypadków i przepisu tego nie można byłoby wykorzystać jako podstawy legalności masowego gromadzenia lub przetwarzania danych osobowych. W sytuacji, w której byłoby to konieczne, art. 7 lit. c) lub e) stanowiłyby odpowiedniejszą podstawę przetwarzania.

III.2.5. Zadanie publiczne

Artykuł 7 lit. e) stanowi podstawę prawną w sytuacjach, w których „przetwarzanie danych 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".

Trzeba zwrócić uwagę, że art. 7 lit. e), podobnie jak art. 7 lit. c), odnosi się do interesu publicznego Unii Europejskiej lub państwa członkowskiego. Podobnie „władza publiczna" oznacza władzę przyznaną przez Unię Europejską lub państwo członkowskie. Innymi słowy, zadania wykonywane w interesie publicznym państwa trzeciego lub w ramach wykonywania

władzy publicznej nadanej na mocy prawa zagranicznego nie wchodzą w zakres stosowania tego przepisu[41].

Artykuł 7 lit. e) obejmuje dwie sytuacje i odnosi się zarówno do sektora publicznego, jak i do sektora prywatnego. Po pierwsze, obejmuje sytuacje, w których sam administrator danych ma władzę publiczną lub zadanie leżące w interesie publicznym (ale niekoniecznie spoczywa na nim również zobowiązanie prawne do przetwarzania danych) i przetwarzanie jest konieczne dla wykonywania tej władzy lub tego zadania. Na przykład organ podatkowy może gromadzić i przetwarzać zeznania podatkowe danej osoby w celu ustalenia i zweryfikowania kwoty podatku do zapłacenia lub stowarzyszenia zawodowe, takie jak izby adwokackie lub lekarskie, mogą przeprowadzać procedury dyscyplinarne wobec niektórych swoich członków, jeżeli przyznano im taką władzę publiczną. Jeszcze innym przykładem mogą być jednostki samorządu terytorialnego, takie jak władze gminy, którym powierzono zadanie polegające na świadczeniu usług przez bibliotekę, szkołę lub lokalną pływalnię.

Po drugie, art. 7 lit. e) obejmuje również sytuacje, w których administrator danych nie ma władzy publicznej, ale osoba trzecia, która ma taką władzę, zwróciła się do niego o ujawnienie danych. Na przykład urzędnik organu publicznego właściwego do prowadzenia dochodzeń w sprawie przestępstw może poprosić administratora danych o współpracę w prowadzonym dochodzeniu zamiast nakazać administratorowi danych zastosowanie się do konkretnego żądania współpracy. Artykuł 7 lit. e) może ponadto obejmować sytuacje, w których administrator danych aktywnie ujawnia dane osobie trzeciej mającej taką władzę publiczną. Może to mieć miejsce na przykład w przypadku, gdy administrator danych stwierdzi, że popełniono przestępstwo, i z własnej inicjatywy udostępnia te informacje właściwym organom ścigania.

W przeciwieństwie do sytuacji objętej art. 7 lit. c) w tym przypadku na administratorze danych nie spoczywa wymóg działania na mocy zobowiązania prawnego. W powyższym przykładzie administrator danych, który przypadkowo zauważył, że popełniono kradzież lub oszustwo, może nie być prawnie zobowiązany poinformować o tym policję, ale w stosownych przypadkach może jednak to zrobić dobrowolnie na podstawie art. 7 lit. e).

Przetwarzanie musi być jednak „konieczne dla realizacji zadania wykonywanego w interesie publicznym". Ewentualnie administrator danych lub osoba trzecia, której administrator ten ujawnia dane, muszą mieć władzę publiczną, a przetwarzanie danych musi być konieczne dla wykonywania tej władzy[42]. Trzeba również podkreślić, że tę władzę publiczną lub zadanie publiczne zazwyczaj przypisuje się w przepisach ustawowych lub innych regulacjach prawnych. Jeśli przetwarzanie wiąże się z naruszeniem prywatności lub jeżeli na mocy prawa krajowego wymagane jest zapewnienie ochrony zainteresowanych osób, podstawa prawna powinna być wystarczająco szczegółowa i precyzyjna pod względem określenia rodzaju przetwarzania danych, które może być dozwolone.

Takie sytuacje występują coraz częściej, również poza granicami sektora publicznego, zważywszy tendencję do outsourcingu zadań rządowych na rzecz podmiotów w sektorze

[41] Zob. podobna interpretacja pojęcia „ważnych względów publicznych" zawartego w art. 26 ust. 1 lit. d) dyrektywy, przedstawiona w sekcji 2.4 dokumentu roboczego Grupy Roboczej w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r., przyjętego w dniu 25 listopada 2005 r. (WP114).

[42] Innymi słowy, w tych przypadkach znaczenie publiczne zadań i związana z nimi odpowiedzialność nadal będą istniały, nawet jeżeli wykonywanie danego zadania powierzono innym podmiotom, w tym prywatnym.

prywatnym. Może to mieć miejsce na przykład w kontekście działalności związanej z przetwarzaniem w sektorze transportu lub zdrowia (m.in. w ramach badań epidemiologicznych i innych). Na podstawę tę można również powołać się w kontekście egzekwowania prawa, jak już zasugerowano w przykładach powyżej. Stopień przyzwolenia przedsiębiorstwu prywatnemu na współpracę z organami ścigania, na przykład w zakresie zwalczania oszustw lub nielegalnych treści w Internecie, wymaga analizy nie tylko na mocy art. 7, ale również na mocy art. 6, biorąc pod uwagę wymogi celowości, legalności i rzetelności[43].

Artykuł 7 lit. e) ma potencjalnie bardzo szeroki zakres stosowania, który wymaga ścisłej wykładni oraz jasnego określenia w poszczególnych przypadkach przedmiotowego interesu publicznego oraz władzy publicznej uzasadniającej przetwarzanie. Ten szeroki zakres wyjaśnia również, dlaczego – dokładnie jak w przypadku art. 7 lit. f) – w art. 14 przewidziano prawo sprzeciwu, gdy podstawą przetwarzania jest art. 7 lit. e)[44]. W obu przypadkach mogą zatem stosować się podobne dodatkowe gwarancje i środki[45].

W tym sensie art. 7 lit. e) wykazuje podobieństwo do art. 7 lit. f), a w pewnym kontekście, zwłaszcza w odniesieniu do organów publicznych, art. 7 lit. e) może zastępować art. 7 lit. f).

Przy ocenie zakresu stosowania tych przepisów do podmiotów sektora publicznego, w szczególności w świetle proponowanych zmian ram prawnych w zakresie ochrony danych, warto zwrócić uwagę, że w obecnym tekście rozporządzenia (WE) nr 45/2001[46], które zawiera przepisy o ochronie danych mające zastosowanie do instytucji i organów Unii Europejskiej, nie ma przepisu porównywalnego z art. 7 lit. f).

Motyw 27 tego rozporządzenia stanowi jednak, że „Przetwarzanie danych osobowych w celu przeprowadzenia czynności wykonywanych *w interesie ogólnym* przez instytucje i organy wspólnotowe obejmuje przetwarzanie danych osobowych niezbędnych dla zarządzania i funkcjonowania tych instytucji i organów". Przepis ten pozwala zatem na przetwarzanie danych na podstawie szeroko interpretowanego „zadania publicznego" w wielu różnych przypadkach, które w innym razie mogłyby być objęte przepisem podobnym do art. 7 lit. f). Nadzór wideo pomieszczeń w celach bezpieczeństwa, elektroniczne monitorowanie poczty e-mail czy ocena pracowników to tylko kilka przykładów tego, co może wchodzić w zakres tych szeroko interpretowanych „zadań wykonywanych w interesie publicznym".

Patrząc w przyszłość, trzeba również wziąć pod uwagę, że w art. 6 ust. 1 lit. f) proponowanego rozporządzenia wyraźnie przewiduje się, że podstawa dotycząca uzasadnionego interesu „nie stosuje się do przetwarzania realizowanego przez organy publiczne w wykonaniu ich zadań". Jeśli przepis ten wejdzie w życie i będzie interpretowany

[43] Zob. w tym kontekście opinia Grupy Roboczej w sprawie SWIFT (przywołana w przypisie 39 powyżej), opinia 4/2003 Grupy Roboczej w sprawie poziomu ochrony zapewnianej przez Stany Zjednoczone przy przekazywaniu danych pasażerów, przyjęta 13.06.2003 r. (WP78), oraz dokument roboczy w sprawie zagadnień ochrony danych związanych z prawem własności intelektualnej, przyjęty 18.01.2005 r. (WP 104).

[44] Jak wspomniano powyżej, ta możliwość sprzeciwu nie istnieje w niektórych państwach członkowskich (np. w Szwecji) w odniesieniu do przetwarzania danych na podstawie art. 7 lit. e).

[45] Jak zostanie wykazane poniżej, w projekcie sprawozdania komisji LIBE zasugerowano dalsze gwarancje – w szczególności większą przejrzystość – w przypadku gdy zastosowanie ma art. 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 i o swobodnym przepływie takich danych. (Dz.U. L 8 z 12.1.2001, s. 1).

szeroko, tak aby całkowicie uniemożliwić organom publicznym wykorzystywanie uzasadnionego interesu jako podstawy prawnej, wówczas określone w art. 7 lit. e) podstawy dotyczące „interesu publicznego" i „władzy publicznej" trzeba będzie interpretować jako dające organom publicznym pewien stopień elastyczności, przynajmniej w celu zapewnienia ich właściwego zarządzania i funkcjonowania, podobnie jak ma to miejsce w przypadku obecnej wykładni rozporządzenia (WE) nr 45/2001.

Ewentualnie wspomniane ostatnie zdanie art. 6 ust. 1 lit. f) proponowanego rozporządzenia mogłoby być interpretowane w taki sposób, aby nie uniemożliwiać całkowicie organom publicznym wykorzystywania uzasadnionego interesu jako podstawy prawnej. W tym przypadku wyrażenie „przetwarzania realizowane przez organy publiczne w wykonaniu ich zadań" zawarte w proponowanym art. 6 ust. 1 lit. f) należy interpretować zawężająco. Ta wąska wykładnia oznaczałaby, że przetwarzanie na potrzeby właściwego zarządzania tymi organami publicznymi i ich funkcjonowania nie wchodzi w zakres „przetwarzania realizowanego przez organy publiczne w wykonaniu ich zadań". W efekcie przetwarzanie na potrzeby właściwego zarządzania tymi organami publicznymi i ich funkcjonowania mogłoby nadal być możliwe na podstawie uzasadnionego interesu.

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

Artykuł 7 lit. f)[47] wymaga przeprowadzenia testu równowagi: uzasadnione interesy administratora danych (lub osób trzecich) trzeba rozważyć w kontekście interesów lub podstawowych praw i wolności osoby, której dane dotyczą. Wynik tego testu równowagi w dużej mierze przesądza o tym, czy art. 7 lit. f) można traktować jako podstawę prawną przetwarzania.

Warto wspomnieć już na tym etapie, że nie jest to zwykły test równowagi, który polega tylko na zważeniu dwóch łatwo policzalnych i porównywalnych „wag". Jak opisano bardziej szczegółowo poniżej, przeprowadzenie testu równowagi może raczej wymagać złożonej oceny z uwzględnieniem wielu czynników. Aby pomóc w zorganizowaniu i uproszczeniu tej oceny podzielono ten proces na kilka etapów. Służy to zapewnieniu skutecznego przeprowadzenia testu równowagi.

W sekcji III.3.1 przeanalizowano najpierw jedną stronę równowagi: co stanowi „uzasadniony interes administratora danych lub osoby trzeciej, którym dane są ujawniane". W sekcji III.3.2 zbadano drugą stronę równowagi – co stanowi „interesy związane z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1".

W sekcjach III.3.3 i III.3.4 przedstawiono wytyczne dotyczące sposobu przeprowadzenia testu równowagi. Sekcja III.3.3 zawiera ogólne wprowadzenie w postaci trzech różnych scenariuszy. Po tym wprowadzeniu w sekcji III.3.4 przedstawiono najważniejsze czynniki, które trzeba uwzględnić przy przeprowadzaniu testu równowagi, w tym gwarancje i środki zapewnione przez administratora danych.

Ponadto w sekcjach III.3.5 i III.3.6 przeanalizowano również niektóre szczególne mechanizmy, takie jak: rozliczalność, przejrzystość i prawo sprzeciwu, które mogą pomóc

[47] Pełny tekst art. 7 lit. f) – zob. s. 5 powyżej.

zapewnić – i umacniać – odpowiednią równowagę różnych przedmiotowych interesów.

III.3.1. Uzasadnione interesy administratora danych (lub osób trzecich)

Pojęcie „interesu”

Pojęcie „interesu” jest ściśle związane z pojęciem „celu”, o którym mowa w art. 6 dyrektywy, lecz różni się od niego. W dyskursie o ochronie danych „cel” jest konkretnym powodem, dla którego dane są przetwarzane: założeniem lub zamiarem przetwarzania danych. Z drugiej strony interes jest szerszym udziałem, który administrator danych może mieć w przetwarzaniu, lub korzyścią, którą administrator danych czerpie – lub którą społeczeństwo może czerpać – z przetwarzania.

Na przykład przedsiębiorstwo może mieć *interes* w zapewnieniu zdrowia i bezpieczeństwa swojego personelu pracującego w swojej elektrowni jądrowej. W związku z tym *celem* tego przedsiębiorstwa może być wdrożenie określonych procedur kontroli dostępu, co uzasadnia przetwarzanie pewnych określonych danych osobowych, aby przyczynić się do zapewnienia zdrowia i bezpieczeństwa pracowników.

Interes musi być wystarczająco jasno sformułowany, aby umożliwić przeprowadzenie testu równowagi w odniesieniu do interesów i praw podstawowych osoby, której dane dotyczą. Ponadto przedmiotowy interes musi być także interesem „administratora danych”. Wymaga to rzeczywistego i aktualnego interesu, czegoś, co odpowiada bieżącym działaniom lub korzyściom, które są oczekiwane w bardzo bliskiej przyszłości. Innymi słowy, interesy, które są zbyt ogólnikowe lub oparte na przypuszczeniach, będą niewystarczające.

Charakter interesu może być różny. Niektóre interesy mogą być ważne i korzystne dla ogółu społeczeństwa, jak na przykład interes prasy dotyczący publikowania informacji na temat korupcji rządu lub interes dotyczący prowadzenia badań naukowych (z zastrzeżeniem odpowiednich gwarancji). Inne interesy mogą być mniej pilne dla całego społeczeństwa lub w każdym razie wpływ realizacji tych interesów na społeczeństwo może mieć charakter bardziej mieszany lub kontrowersyjny. Może to na przykład odnosić się do interesu gospodarczego przedsiębiorstwa polegającego na zdobyciu jak najszerszej wiedzy o potencjalnych klientach, tak aby mogło ono lepiej ukierunkować reklamy swoich produktów lub usług.

Co sprawia, że interes jest „uzasadniony” lub „nieuzasadniony”?

Celem tego pytania jest ustalenie progu tego, co stanowi uzasadniony interes. Jeżeli interes administratora danych jest nieuzasadniony, test równowagi nie będzie wchodził w grę, gdyż początkowy próg stosowania art. 7 lit. f) nie zostanie osiągnięty.

Zdaniem Grupy Roboczej pojęcie uzasadnionego interesu mogłoby obejmować wiele różnych interesów, banalnych lub bardzo ważnych, jasnych lub bardziej kontrowersyjnych. W ramach drugiego etapu, jeżeli chodzi o porównywanie tych interesów z interesami i prawami podstawowymi osób, których dane dotyczą, należy zatem przyjąć bardziej ograniczone podejście i przeprowadzić bardziej merytoryczną analizę.

Poniżej zamieszczono niepełny wykaz pewnych najczęstszych sytuacji, w których może pojawić się kwestia uzasadnionego interesu w rozumieniu art. 7 lit. f). Pozostaje on bez

uszczerbku dla tego, czy w teście równowagi interesy administratora danych w końcu przeważą nad interesami i prawami osób, których dane dotyczą.

- Korzystanie z prawa do wolności wypowiedzi i informacji, w tym w mediach i sztuce
- Konwencjonalny marketing bezpośredni i inne formy marketingu lub reklamy
- Niezamówione wiadomości niehandlowe, w tym na potrzeby kampanii politycznych lub zbierania środków na cele charytatywne
- Egzekwowanie roszczeń prawnych, w tym windykacja należności w drodze postępowania pozasądowego
- Zapobieganie oszustwom, niewłaściwemu wykorzystywaniu usług lub praniu pieniędzy
- Monitorowanie pracowników dla celów bezpieczeństwa lub zarządzania
- Systemy informowania o nieprawidłowościach
- Bezpieczeństwo fizyczne, bezpieczeństwo informatyczne i bezpieczeństwo sieci
- Przetwarzanie w celach historycznych, naukowych lub statystycznych
- Przetwarzanie do celów badań naukowych (w tym badań marketingowych)

W związku z tym interes można uznać za uzasadniony, o ile administrator danych może realizować ten interes w sposób, który jest zgodny z przepisami o ochronie danych i innymi przepisami. Innymi słowy, uzasadniony interes musi być „dopuszczalny na mocy prawa”[48].

Aby „uzasadniony interes” miał znaczenie na mocy art. 7 lit. f), musi więc:

- być legalny (tj. zgodny z mającym zastosowanie prawem UE i krajowym);
- być dostatecznie jasno sformułowany, aby umożliwić przeprowadzenie testu równowagi w odniesieniu do interesów i praw podstawowych osoby, której dane dotyczą (tj. wystarczająco szczegółowy);
- stanowić rzeczywisty i aktualny interes (tj. nie może być oparty na przypuszczeniach).

Fakt, że administrator danych ma taki uzasadniony interes w przetwarzaniu pewnych danych, nie oznacza, że może koniecznie powoływać się na art. 7 lit. f) jako podstawę prawną przetwarzania. Legalność interesu administratora danych jest tylko punktem wyjścia, jednym z elementów, które trzeba przeanalizować na mocy art. 7 lit. f). To, czy można powoływać się na art. 7 lit. f), będzie zależało od wyniku testu równowagi, który zostanie przeprowadzony później.

[48] Uwagi na temat charakteru „legalności” zawarte w sekcji III.1.3 opinii 3/2013 Grupy Roboczej w sprawie celowości (przywołanej w przypisie 9 powyżej) stosują się odpowiednio również w tym przypadku. Jak stwierdza się w tej opinii na s. 19–20, pojęcie „prawa” jest tu używane w najszerszym znaczeniu. Obejmuje to inne mające zastosowanie przepisy, takie jak prawo pracy, prawo zobowiązań lub prawo ochrony konsumentów. Ponadto pojęcie prawa „obejmuje wszystkie formy prawa pisanego i zwyczajowego, prawa pierwotnego i wtórnego, dekretów gminnych, precedensów sądowych, zasad konstytucyjnych, praw podstawowych, innych zasad prawnych, jak również orzecznictwo, gdyż takie »prawa« byłyby interpretowane i uwzględniane przez właściwe sądy. W ramach prawa inne elementy, takie jak: zwyczaje, kodeksy postępowania, kodeksy etyki, ustalenia umowne, a także ogólny kontekst i okoliczności danego przypadku, również mogą być brane pod uwagę przy ustalaniu, czy dany cel jest uzasadniony. Obejmie to charakter podstawowej relacji między administratorem danych a osobami, których dane dotyczą, czy będzie to relacja handlowa, czy inna”. Ponadto to, co można uznać za uzasadniony interes, „może zmieniać się w czasie w zależności od postępu naukowego i technologicznego oraz zmian w społeczeństwie i w postawach kulturowych”.

Przykład: administratorzy danych mogą mieć uzasadniony interes leżący w poznaniu preferencji swoich klientów, tak aby mogli lepiej spersonalizować swoje oferty i ostatecznie oferować produkty i usługi, które lepiej zaspokajają potrzeby i pragnienia klientów. W tym świetle art. 7 lit. f) może być odpowiednią podstawą prawną, którą można stosować w przypadku niektórych rodzajów działalności marketingowej, w Internecie i poza nim, pod warunkiem że wprowadzone są odpowiednie gwarancje (w tym między innymi sprawny mechanizm umożliwiający wyrażenie sprzeciwu wobec takiego przetwarzania na mocy art. 14 lit. b), co zostanie omówione w sekcji III.3.6 *Prawo sprzeciwu oraz dalsze czynniki*).

Nie oznacza to jednak, że administratorzy danych mogliby powoływać się na art. 7 lit. f), aby bezpodstawnie monitorować działania swoich klientów w Internecie i poza nim, łączyć ogromne ilości danych o nich z różnych źródeł, które to dane początkowo gromadzono w innych kontekstach i dla różnych celów, oraz tworzyć złożone profile osobowości i preferencji klientów bez ich wiedzy, sprawnego mechanizmu sprzeciwu, nie mówiąc już o świadomej zgodzie – i także handlować tymi profilami, na przykład za pośrednictwem brokerów danych. Takie profilowanie prawdopodobnie stanowiłoby znaczącą ingerencję w prywatność klienta, a w takim przypadku interesy i prawa osoby, której dane dotyczą, byłyby nadrzędne względem interesu administratora danych[49].

Inny przykład: w swojej opinii w sprawie SWIFT[50] Grupa Robocza stwierdziła, że chociaż przedsiębiorstwo to ma uzasadniony interes w stosowaniu się do wezwań do sądu na mocy prawa Stanów Zjednoczonych, aby uniknąć ryzyka nałożenia sankcji przez organy amerykańskie, nie można powoływać się na art. 7 lit. f). Grupa Robocza uznała w szczególności, że ze względu na daleko idące skutki, jakie przetwarzanie danych „w sposób tajny, systematyczny, masowy i przez długi czas" ma dla osób fizycznych, „interesy wynikające z podstawowych praw i wolności licznej grupy osób, których dane dotyczą, mają pierwszeństwo nad interesem przedsiębiorstwa SWIFT polegającym na uniknięciu sankcji władz amerykańskich w związku z ewentualnym niezastosowaniem się do wezwań".

Jak zostanie pokazane w dalszej części niniejszej opinii, jeśli interes realizowany przez administratora danych nie jest ważny, istnieje większe prawdopodobieństwo, że interesy i prawa osoby, której dane dotyczą, przeważają nad uzasadnionymi – ale mniej istotnymi – interesami administratora danych. Jednocześnie nie znaczy to, że mniej ważne interesy administratora danych nie mogą czasami przeważać nad interesami i prawami osób, których dane dotyczą: zazwyczaj dzieje się tak, gdy wpływ przetwarzania na osoby, których dane dotyczą, również jest mniej istotny.

Uzasadniony interes w sektorze publicznym

[49] Kwestia technologii śledzenia i rola zgody na mocy art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej zostaną omówione oddzielnie. Zob. sekcja III.3.6 lit. b), „Przykład: ewolucja podejścia do marketingu bezpośredniego".

[50] Zob. sekcja 4.2.3 tej opinii, przywołanej już w przypisie 39 powyżej. Uzasadniony interes administratora danych w tym przypadku był również związany z interesem publicznym państwa trzeciego, którego to interesu nie można było uwzględnić na mocy dyrektywy 95/46/WE.

W obecnym tekście dyrektywy nie wyklucza się wyraźnie administratorów danych, którzy są organami publicznymi, z przetwarzania danych z wykorzystaniem art. 7 lit. f) jako podstawy prawnej przetwarzania[51].

W proponowanym rozporządzeniu[52] wyklucza się jednak tę możliwość w przypadku „przetwarzania realizowanego przez organy publiczne w wykonaniu ich zadań".

Proponowana zmiana legislacyjna uwydatnia znaczenie ogólnej zasady, zgodnie z którą organy publiczne powinny przetwarzać dane w ramach wykonywania swoich zadań tylko wtedy, gdy mają na to odpowiednie zezwolenie na mocy prawa. Przestrzeganie tej zasady jest szczególnie ważne – i wyraźnie wymagane w orzecznictwie Europejskiego Trybunału Praw Człowieka – w przypadkach, w których zagrożona jest prywatność osób, których dane dotyczą, a działalność organu publicznego stanowiłyby ingerencję w tę prywatność.

Wystarczająco *szczegółowe i szczególne* zezwolenie na podstawie prawa jest zatem wymagane – także na mocy obecnej dyrektywy – w przypadku gdy przetwarzanie przez organy publiczne ingeruje w prywatność osób, których dane dotyczą. Może to mieć formę konkretnego zobowiązania prawnego do przetwarzania danych, które może odpowiadać wymogom art. 7 lit. c), albo szczególnego zezwolenia (ale niekoniecznie obowiązku) na przetwarzanie danych, które może spełniać wymogi art. 7 lit. e) lub f)[53].

Uzasadnione interesy osób trzecich

Obecny tekst dyrektywy nie tylko odnosi się do „uzasadnionych interesów administratora danych", ale także pozwala stosować art. 7 lit. f) w przypadku uzasadnionych interesów „osoby trzeciej, lub osobom, którym dane są ujawniane"[54]. Poniższe przykłady ilustrują pewne konteksty, w których ten przepis może mieć zastosowanie.

Publikacja danych dla celów przejrzystości i rozliczalności. Jednym z ważnych kontekstów, w których art. 7 lit. f) może być istotny, jest przypadek publikacji danych dla celów przejrzystości i rozliczalności (na przykład danych dotyczących wynagrodzenia kadry

[51] Pierwotnie pierwszy wniosek Komisji dotyczący dyrektywy obejmował oddzielnie przetwarzanie danych w sektorze prywatnym i przetwarzanie w sektorze publicznym. To formalne rozróżnienie między przepisami mającymi zastosowanie do sektora publicznego i do sektora prywatnego porzucono w zmienionym wniosku. Mogło to również doprowadzić do różnic w wykładni i wdrażaniu przepisów przez poszczególne państwa członkowskie.

[52] Zob. art. 6 ust. 1 lit. f) proponowanego rozporządzenia.

[53] Pod tym względem zob. także sekcja III.2.5. powyżej na temat zadań publicznych (s. 23–26) oraz dyskusja poniżej w punkcie *Uzasadnione interesy osób trzecich* (s. 30–31). Zob. także rozważania na temat ograniczeń „egzekwowania prawa na drodze prywatnoprawnej" na s. 40 w punkcie „Interesy publiczne/interesy szerszej społeczności". We wszystkich tych sytuacjach szczególnie istotne jest zapewnienie pełnego poszanowania ograniczeń zawartych w art. 7 lit. f) i e).

[54] Celem zaproponowanego rozporządzenia jest ograniczenie stosowania tej podstawy w odniesieniu do „słusznych interesów realizowanych przez administratora". Z samego tekstu nie wynika jasno, czy proponowany język oznacza zwykłe uproszczenie treści, czy jego celem jest wykluczenie sytuacji, w których administrator danych mógłby ujawnić dane w uzasadnionym interesie innych. Ten tekst nie jest jednak ostateczny. Interes osób trzecich został na przykład ponownie umieszczony w sprawozdaniu końcowym komisji LIBE przy okazji głosowania nad kompromisowymi poprawkami komisji LIBE Parlamentu Europejskiego w dniu 21 października 2013 r. Zob. poprawka 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.

kierowniczej wyższego szczebla w przedsiębiorstwie). W tym przypadku można uznać, że publiczne ujawnienie odbywa się przede wszystkim nie w interesie administratora danych, który publikuje dane, ale raczej w interesie innych zainteresowanych stron, takich jak: pracownicy, dziennikarze lub ogół społeczeństwa, którym dane zostają ujawnione.

Z punktu widzenia ochrony danych i prywatności, a także w celu zapewnienia pewności prawa, na ogół wskazane jest podawanie danych osobowych do wiadomości publicznej na podstawie ustawy, w której pozwala się na publikowanie danych oraz w której w stosownych przypadkach wyraźnie określa się dane, które mają być opublikowane, cele publikacji oraz wszelkie niezbędne gwarancje[55]. Oznacza to również, że w przypadku gdy dane osobowe są ujawniane dla celów przejrzystości i rozliczalności, lepszą podstawę prawną może stanowić art. 7 lit. c), a nie art. 7 lit. f)[56].

W przypadku braku określonego zobowiązania prawnego lub zgody na publikację danych mogłoby jednak być możliwe ujawnienie danych osobowych zainteresowanym stronom. W stosownych przypadkach byłoby również możliwe opublikowanie danych osobowych dla celów przejrzystości i rozliczalności.

W obu przypadkach – tj. niezależnie od tego, czy dane osobowe ujawnia się na podstawie ustawy to umożliwiającej – ujawnienie bezpośrednio zależy od wyniku testu równowagi na mocy art. 7 lit. f) oraz od wprowadzenia odpowiednich gwarancji i środków[57].

Ponadto pożądane może być również dalsze wykorzystywanie już ujawnionych danych osobowych dla celów jeszcze większej przejrzystości (na przykład ponowna publikacja danych przez prasę lub dalsze rozpowszechnianie pierwotnie opublikowanego zbioru danych przez organizację pozarządową w sposób bardziej innowacyjny i przyjazny dla użytkownika). To, czy takie ponowne opublikowanie i ponowne wykorzystanie jest możliwe, będzie również zależało od wyniku testu równowagi, w którym należy uwzględnić między innymi charakter informacji i skutek ponownej publikacji lub ponownego wykorzystania dla osób fizycznych[58].

[55] To zalecenie w sprawie najlepszych praktyk nie powinno naruszać krajowych przepisów prawa dotyczących przejrzystości i publicznego dostępu do dokumentów.

[56] W niektórych państwach członkowskich istnieją różne przepisy, których należy przestrzegać w odniesieniu do przetwarzania danych przez podmioty publiczne i prywatne. Na przykład zgodnie z włoskim kodeksem ochrony danych osobowych rozpowszechnianie danych osobowych przez organ publiczny dozwolone jest wyłącznie w przypadkach przewidzianych w przepisach ustawowych lub wykonawczych (sekcja 19.3).

[57] Jak wyjaśniono w opinii 06/2013 Grupy Roboczej w sprawie otwartych danych (zob. s. 9 tej opinii, przytoczonej w przypisie 88 poniżej), „przepisy krajowe muszą być zgodne z art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (»EKPC«) oraz art. 7 i art. 8 Karty praw podstawowych Unii Europejskiej (»Karta praw podstawowych UE«). 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". Zob. wyrok Trybunału Sprawiedliwości z dnia 20 maja 2003 r. w sprawach połączonych C-465/00, C-138/01 i C-139/01 Rundfunk oraz wyrok Trybunału Sprawiedliwości z dnia 9 listopada 2010 r. w sprawach połączonych C-92/09 i C-93/09 Volker und Markus Schecke.

[58] Ważnym czynnikiem jest w tym przypadku również celowość. Na s. 22–23 opinii 06/2013 Grupy Roboczej w sprawie otwartych danych (przytoczonej w przypisie 88 poniżej) Grupa Robocza 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

Badania naukowe historyczne lub innego rodzaju. Inny ważny kontekst, w którym istotne może być ujawnienie w uzasadnionych interesach osób trzecich, stanowią badania naukowe – historyczne lub innego rodzaju – zwłaszcza w przypadku gdy wymagany jest dostęp do pewnych baz danych. W dyrektywie wyraźnie uwzględniono takie działania, z zastrzeżeniem odpowiednich gwarancji i środków[59], ale nie należy zapominać, że uzasadnioną podstawą tych działań często będzie przemyślane zastosowanie art. 7 lit. f)[60].

Ogólny interes publiczny lub interes osoby trzeciej. Ponadto uzasadniony interes osób trzecich może mieć znaczenie również w inny sposób. Jest to przypadek, w którym administrator danych – czasami zachęcany przez organy publiczne – realizuje interes, który odpowiada ogólnemu interesowi publicznemu lub interesowi osoby trzeciej. Może to obejmować sytuacje, w których administrator danych wykracza poza swoje konkretne zobowiązania prawne określone w przepisach ustawowych i wykonawczych w celu wsparcia organów ścigania lub prywatnych zainteresowanych stron w ich wysiłkach na rzecz zwalczania nielegalnych działań, takich jak: pranie pieniędzy, nagabywanie dzieci dla celów seksualnych lub nielegalne udostępnianie plików w Internecie. W takich sytuacjach szczególnie ważne jest jednak zapewnienie pełnego poszanowania granic określonych w art. 7 lit. f)[61].

Przetwarzanie musi być konieczne dla przewidzianego celu lub celów

Ponadto przetwarzanie danych osobowych musi być „konieczne dla potrzeb wynikających z uzasadnionych interesów" administratora danych lub – w przypadku ujawniania – osoby trzeciej. Warunek ten uzupełnia wymóg konieczności na mocy art. 6 i wymaga istnienia związku między przetwarzaniem a interesami. Ten wymóg „konieczności" ma zastosowanie we wszystkich sytuacjach wymienionych w art. 7 lit. b)–f), ale w przypadku lit. f) szczególnie istotne jest zapewnienie, aby przetwarzanie danych w oparciu o uzasadnione interesy nie prowadziło do nadmiernie szerokiej interpretacji konieczności przetwarzania danych. Tak jak w innych przypadkach oznacza to, że należy rozważyć, czy dostępne są inne, mniej inwazyjne środki służące realizacji tego samego celu.

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

Interesy lub prawa (a nie interesy związane z prawami)

W art. 7 lit. f) dyrektywy mowa jest o interesach podporządkowanych „interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1".

---

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] Zob. np. art. 6 ust. 1 lit. b) i e).

[60] Jak wyjaśniono w opinii 3/2013 Grupy Roboczej w sprawie celowości (przytoczonej w przypisie 9 powyżej), dalsze wykorzystanie danych dla wtórnych celów musi być przedmiotem podwójnego testu. Po pierwsze, należy zapewnić, aby dane były przetwarzane w zgodnych celach. Po drugie, powinno się zapewnić istnienie odpowiedniej podstawy prawnej przetwarzania na mocy art. 7.

[61] W tym kontekście zob. np. dokument roboczy w sprawie zagadnień ochrony danych związanych z prawem własności intelektualnej, przyjęty 18.01.2005 r. (WP 104).

Grupa Robocza zauważyła jednak, porównując różne wersje językowe dyrektywy, że wyrażenie „interests for" przetłumaczono w innych kluczowych językach, którymi posługiwano się podczas negocjowania tekstu dyrektywy, w sposób oddający wyrażenie „interests or"[62].

Dalsza analiza wskazuje na to, że tekst dyrektywy w języku angielskim jest po prostu wynikiem błędu ortograficznego: zamiast „or" napisano „for"[63]. Prawidłowy tekst powinien zatem brzmieć „interests or fundamental rights and freedoms".

„Interesy" i „prawa" należy interpretować szeroko

Odniesienie do „interesów lub podstawowych praw i wolności" ma bezpośredni wpływ na zakres stosowania tego przepisu. Zapewnia on większą ochronę osobie, której dane dotyczą, a mianowicie wymaga uwzględnienia również „interesów" osób, których dane dotyczą, a nie tylko ich podstawowych praw i wolności. Nie ma jednak powodu zakładać, że zawarte w art. 7 lit. f) ograniczenie do praw podstawowych „które gwarantują ochronę na podstawie art. 1 ust. 1" – a zatem wyraźne odniesienie do przedmiotu dyrektywy[64] – nie stosuje się również do terminu „interesy". Istnieje jednak jasne przesłanie, że należy wziąć pod uwagę wszystkie istotne interesy osoby, której dane dotyczą.

Ta wykładnia tekstu ma sens nie tylko pod względem gramatyki, ale również przy uwzględnieniu szerokiej wykładni pojęcia „uzasadnionych interesów" administratora danych. Jeżeli administrator danych – lub osoba trzecia w przypadku ujawnienia – może realizować jakiekolwiek interesy, pod warunkiem że nie są one nieuzasadnione, to osoba, której dane dotyczą, również powinna mieć prawo do tego, żeby uwzględniono wszystkie kategorie jej interesów i porównano je z interesami administratora danych, o ile interesy tej osoby są istotne w zakresie stosowania dyrektywy.

W czasach postępującego braku równowagi w zakresie „władzy nad informacjami", kiedy zarówno rządy, jak i organizacje przedsiębiorstw gromadzą dotychczas niespotykane ilości danych na temat osób fizycznych i mają coraz większe możliwości pod względem opracowywania szczegółowych profilów, które przewidują zachowanie tych osób (co powiększa tę nierównowagę informacyjną i ogranicza niezależność tych osób), coraz ważniejsze jest zapewnienie ochrony interesów osób fizycznych w zakresie zachowania ich prywatności i niezależności.

---

[62] Na przykład „l'intérêt ou les droits et libertés fondamentaux de la personne concernée" w języku francuskim; „l'interesse o i diritti e le libertà fondamentali della persona interessata" w języku włoskim; „das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person" w języku niemieckim.

[63] Grupa Robocza zwraca uwagę, że gramatycznie poprawna wersja angielska powinna brzmieć „interests in", a nie „interests for", jeżeli to miano na myśli. Dodatkowo wyrażenie „interests for" lub „interests in" wydaje się po pierwsze zbędne, ponieważ odwołanie do „podstawowych praw oraz wolności" powinno w normalnych warunkach wystarczyć, jeżeli to miano na myśli. Interpretację, że doszło do błędu ortograficznego, potwierdza również fakt, że we wspólnym stanowisku (WE) nr 1/95, przyjętym przez Radę dnia 20 lutego 1995 r. również odwołano się do „interests or fundamental rights and freedoms". Ponadto Grupa Robocza zwraca także uwagę, że Komisja zamierzała poprawić ten błąd we wniosku dotyczącym rozporządzenia: art. 6 ust. 1 lit. f) zawiera odniesienie do „the interests or fundamental rights and freedoms of the data subject which require protection of personal data" („interesów lub podstawowych praw i wolności osoby, której dane dotyczą, które gwarantują ochronę danych osobowych"), a nie do „interests for" („interesów związanych z") w odniesieniu do tych praw.

[64] Zob. 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".

Trzeba również zwrócić uwagę, że w przypadku osób, których dane dotyczą, słowa „interesy" nie poprzedzono przymiotnikiem „uzasadnione", który zastosowano natomiast do interesów administratora danych. Oznacza to szerszy zakres do ochrony interesów i praw osób fizycznych. Nawet osoby fizyczne zaangażowane w nielegalną działalność nie powinny doświadczać nieproporcjonalnej ingerencji w ich prawa i interesy[65]. Na przykład interesy osoby, która być może dopuściła się kradzieży w supermarkecie, nadal mogą być ważniejsze niż opublikowanie jej zdjęcia i prywatnego adresu na ścianie supermarketu lub w Internecie przez właściciela sklepu.

III.3.3. Wprowadzenie do stosowania testu równowagi

Przydatne jest wyobrażenie sobie zarówno uzasadnionych interesów administratora danych, jak i wpływu na interesy i prawa osoby, której dane dotyczą, w postaci spektrum. Uzasadnione interesy mogą dotyczyć spektrum interesów: od mało znaczących, przez dość ważne, do ważnych. Podobnie wpływ na interesy i prawa osób, których dane dotyczą, może być bardziej lub mniej znaczący i może mieć rozpiętość od banalnego po bardzo poważny.

Uzasadnione interesy administratora danych, jeżeli są mało znaczące i niezbyt ważne, mogą na ogół być nadrzędne wobec interesów i praw osób, których dane dotyczą, wyłącznie w sytuacjach, w których wpływ na te prawa i interesy jest jeszcze bardziej banalny. Z drugiej strony istotne i ważne uzasadnione interesy mogą w niektórych przypadkach oraz z zastrzeżeniem gwarancji i środków uzasadniać nawet znaczną ingerencję w prywatność lub inny istotny wpływ na interesy i prawa osób, których dane dotyczą[66].

Trzeba w tym miejscu podkreślić szczególną rolę, którą gwarancje mogą odgrywać[67] pod względem zmniejszenia nadmiernego wpływu na osoby, których dane dotyczą, a tym samym zmienienia równowagi praw i interesów w takim stopniu, że uzasadnione interesy administratora danych nie będą podrzędne. Samo stosowanie gwarancji oczywiście nie wystarcza, żeby uzasadnić każdy rodzaj przetwarzania we wszystkich kontekstach. Ponadto gwarancje te muszą być odpowiednie i wystarczające oraz muszą niewątpliwie i znacznie zmniejszać wpływ na osoby, których dane dotyczą.

---

[65] Oczywiście jedną z konsekwencji przestępczości może być gromadzenie oraz możliwa publikacja danych osobowych na temat przestępców i podejrzanych. Musi to jednak podlegać rygorystycznym warunkom i gwarancjom.

[66] Zob. jako przykład 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 z dnia 20 listopada 2005 r. (wniosek w sprawie kontroli chorób zakaźnych 42 CFR część 70 i 71), przyjęta 14.06.2006 r. (WP 121), w której mowa o określonych poważnych zagrożeniach dla zdrowia publicznego;
- opinia 1/2006 w sprawie wewnętrznych systemów informowania o nieprawidłowościach (przywołana powyżej w przypisie 39), w której 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), w którym wyważono prawo pracodawcy do efektywnego prowadzenia działalności względem godności ludzkiej pracownika, jak również poufności korespondencji.

[67] Gwarancje 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 rozdziału funkcjonalnego, odpowiednie wykorzystywanie technik anonimizacji, agregację danych oraz technologie służące wzmocnieniu ochrony prywatności, ale również zwiększoną przejrzystość, rozliczalność oraz możliwość rezygnacji z przetwarzania. Zob. także sekcja III.3.4 lit. d) i nast.

Scenariusze wprowadzające

Przed przejściem do wytycznych dotyczących sposobu przeprowadzenia testu równowagi następujące trzy scenariusze wprowadzające mogą stanowić pierwszą ilustrację tego, jak równoważenie interesów i praw może wyglądać w rzeczywistości. Wszystkie trzy przykłady opierają się na prostym, niewinnym scenariuszu, który rozpoczyna się od specjalnej oferty dotyczącej włoskiej kuchni na wynos. W przykładach stopniowo wprowadzane są nowe elementy, które pokazują, w jaki sposób przechyla się szala w miarę wzrostu wpływu na osoby, których dane dotyczą.

Scenariusz 1: oferta specjalna sieci pizzerii

Claudia zamawia pizzę za pośrednictwem aplikacji mobilnej na swoim smartfonie, ale na stronie internetowej nie korzysta z opcji rezygnacji z otrzymywania informacji marketingowych. Jej adres i dane karty kredytowej są przechowywane na potrzeby dostawy. Kilka dni później do skrzynki pocztowej w domu Claudii przychodzą kupony rabatowe na podobne produkty od sieci pizzerii.

Krótka analiza: sieć pizzerii ma uzasadniony, ale nie szczególnie ważny, interes, żeby spróbować sprzedać swoim klientom więcej produktów. Z drugiej strony, nie wydaje się, aby dochodziło do istotnej ingerencji w prywatność Claudii lub jakiegokolwiek innego nadmiernego wpływu na jej interesy i prawa. Dane i kontekst są stosunkowo niewinne (konsumpcja pizzy). Sieć pizzerii ustanowiła pewne gwarancje: wykorzystywane są tylko dość ograniczone informacje (dane kontaktowe), a kupony przesyłane są pocztą tradycyjną. Ponadto zapewniona jest możliwość łatwego zrezygnowania z otrzymywania informacji marketingowych na stronie internetowej.

W sumie, biorąc również pod uwagę wprowadzone gwarancje i środki (w tym łatwe w użyciu narzędzie umożliwiające rezygnację), interesy i prawa osoby, której dane dotyczą, nie wydają się być nadrzędne wobec uzasadnionego interesu sieci pizzerii leżącego w przetwarzaniu tej minimalnej ilości danych.

Scenariusz 2: ukierunkowana reklama dotycząca tej samej oferty specjalnej

Kontekst jest taki sam, ale tym razem sieć pizzerii przechowuje nie tylko adres Claudii i dane jej karty kredytowej, lecz także najnowszą historię złożonych przez nią zamówień (w ciągu ostatnich trzech lat). Ponadto historia zakupów jest połączona z danymi z supermarketu, w którym Claudia robi zakupy przez Internet, a który prowadzi to samo przedsiębiorstwo, co prowadzące sieć pizzerii. Claudia otrzymuje od sieci pizzerii specjalne oferty i ukierunkowaną reklamę w oparciu o jej historię zamówień dotyczących dwóch różnych usług. Otrzymuje reklamy i oferty specjalne zarówno drogą elektroniczną, jak i tradycyjną: poprzez pocztę konwencjonalną i elektroniczną oraz lokowanie na stronie internetowej przedsiębiorstwa, a także na stronach internetowych wybranych partnerów (kiedy uzyskuje dostęp do tych stron za pośrednictwem komputera lub telefonu komórkowego). Śledzona jest również jej historia odwiedzin stron internetowych (strumień kliknięć). Za pośrednictwem telefonu komórkowego Claudii śledzone są również jej dane dotyczące lokalizacji. Oprogramowanie analityczne przetwarza te dane i przewiduje preferencje Claudii oraz to, kiedy i gdzie najprawdopodobniej dokona ona większych zakupów, będzie skłonna zapłacić wyższą cenę lub będzie bardziej podatna na określoną wysokość upustu lub kiedy ma najsilniejszą ochotę na swoje ulubione desery lub gotowe dania[68]. Claudię bardzo denerwują reklamy ciągle pojawiające się na jej telefonie komórkowym, gdy sprawdza rozkład jazdy autobusów w drodze do domu. Dotyczą one najnowszych ofert dań na wynos, a Claudia próbuje się oprzeć tym reklamom. Claudia nie była w stanie znaleźć prostego sposobu wyłączenia tych reklam ani przyjaznych dla użytkownika informacji na ten temat, choć przedsiębiorstwo twierdzi, że istnieje obejmujący całą branżę system rezygnacji. Była również zaskoczona, gdy zauważyła, że po przeprowadzce do mniej zamożnej dzielnicy przestała otrzymywać oferty specjalne. W efekcie jej miesięczne wydatki na żywność wzrosły o około 10%. Znajoma osoba bardziej obeznana z nowoczesną techniką pokazała jej pewne spekulacje na blogu internetowym. Twierdzono tam, że supermarket pobierał większą opłatę za zamówienia ze „złych dzielnic" ze względu na to, że w takich przypadkach istnieje statystycznie wyższe ryzyko oszustw związanych z kartami kredytowymi. Przedsiębiorstwo nie skomentowało tego twierdzenia i utrzymywało, że jego polityka zniżek i algorytm ustalania cen są zastrzeżone i nie mogą być ujawniane.

Krótka analiza: dane i kontekst nadal mają stosunkowo niewinny charakter. Skala gromadzenia danych i techniki wykorzystywane do wywierania na Claudię wpływu (w tym różne techniki śledzenia, służące przewidywaniu tego, kiedy i gdzie Claudia będzie miała ochotę na jedzenie, oraz fakt, że Claudia jest wówczas najbardziej podatna na pokusę) stanowią jednak czynniki, które należy uwzględnić przy ocenie wpływu przetwarzania. Brak przejrzystości co do logiki przetwarzania danych przez przedsiębiorstwo, która może prowadzić do faktycznej dyskryminacji cenowej ze względu na miejsce, w którym składa się zamówienie, oraz znaczny potencjalny wpływ finansowy na klientów ostatecznie przechylają szalę nawet w stosunkowo niewinnym kontekście posiłków na wynos i zakupów spożywczych. Zamiast jedynie zaoferowania możliwości zrezygnowania z tego typu profilowania i otrzymywania ukierunkowanych reklam konieczna byłaby świadoma zgoda – na podstawie art. 7 lit. a), ale również na mocy art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. W konsekwencji art. 7 lit. f) nie należy traktować jako podstawy prawnej przetwarzania.

[68] Zob. np. http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-

Scenariusz 3: wykorzystywanie zamówień żywności w celu dostosowania wysokości składek na ubezpieczenie zdrowotne

Sieć sprzedaje dane dotyczące nawyków konsumpcyjnych Claudii w zakresie pizzy, w tym czasu i charakteru zamówień, zakładowi ubezpieczeń, który wykorzystuje je do dostosowania wysokości składek na ubezpieczenie zdrowotne.

Krótka analiza: zakład ubezpieczeń zdrowotnych może mieć uzasadniony interes – w zakresie, w jakim pozwalają na to przepisy mające zastosowanie – leżący w ocenie ryzyka dla zdrowia swoich klientów i pobierania zróżnicowanych składek w zależności od różnych czynników ryzyka. Sposób i skala gromadzenia danych są jednak same w sobie nadmierne. Rozsądny człowiek w sytuacji Claudii najprawdopodobniej nie spodziewałby się, że informacje na temat spożywania przez nią pizzy byłyby wykorzystywane do obliczenia wysokości jej składek na ubezpieczenie zdrowotne.

Oprócz nadmiernego charakteru profilowania i możliwości wyciągnięcia nieprawidłowych wniosków (pizza mogła być zamówiona dla innej osoby), wyprowadzanie danych szczególnie chronionych (danych dotyczących zdrowia) na podstawie danych z pozoru nieszkodliwych (zamówienia posiłków na wynos) przyczynia się do przechylenia szali na stronę interesów i praw osoby, której dane dotyczą. Ponadto przetwarzanie ma również znaczący wpływ finansowy na Claudię.

W sumie w tym konkretnym przypadku interesy i prawa osoby, której dane dotyczą, mają charakter nadrzędny wobec uzasadnionych interesów zakładu ubezpieczeń zdrowotnych. W konsekwencji art. 7 lit. f) nie należy traktować jako podstawy prawnej przetwarzania. Wątpliwe jest również, czy art. 7 lit. a) mógłby być wykorzystany jako podstawa prawna, biorąc pod uwagę nadmierną skalę gromadzenia danych, a być może również ze względu na dalsze szczególne ograniczenia na mocy prawa krajowego.

Powyższe scenariusze i możliwe wprowadzenie wersji z innymi elementami uwydatniają potrzebę zapewnienia ograniczonej liczby kluczowych czynników, które mogą być pomocne w ukierunkowaniu oceny, jak również potrzebę przyjęcia pragmatycznego podejścia, które umożliwia stosowanie praktycznych założeń („praktyczne zasady") opartych przede wszystkim na tym, co rozsądna osoba uważałaby za dopuszczalne w danych okolicznościach („uzasadnione oczekiwania"), oraz opartych na konsekwencjach przetwarzania danych dla osób, których dane dotyczą („wpływ").

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

Państwa członkowskie opracowały szereg przydatnych czynników, które należy uwzględnić przy przeprowadzaniu testu równowagi. Czynniki te omówiono w niniejszej sekcji w

boards:„Najnowsze badania sugerują, że siła woli jest ograniczonym zasobem, który z czasem może być uszczuplony lub uzupełniony.[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. Duże zbiory danych mogą pomóc sprzedawcom dokładnie zrozumieć, jak i kiedy zwrócić się do tej konsumentki, gdy jest najbardziej podatna – szczególnie w świecie ciągłego podłączenia do sieci, kiedy nawet nasze urządzenia są celem oferty sprzedażowej".

następujących czterech punktach: a) ocena uzasadnionego interesu administratora danych, b) wpływ na osoby, których dane dotyczą, c) tymczasowa równowaga i d) dodatkowe gwarancje stosowane przez administratora danych, aby zapobiec nadmiernemu wpływowi na osoby, których dane dotyczą[69].

Aby przeprowadzić test równowagi, należy z jednej strony wziąć pod uwagę przede wszystkim charakter i źródło uzasadnionych interesów, a z drugiej strony wpływ na osoby, których dane dotyczą. W tej ocenie należy już uwzględnić środki, które administrator danych zamierza przyjąć w celu zapewnienia zgodności z dyrektywą (na przykład w celu zapewnienia celowości i proporcjonalności na mocy art. 6 lub w celu udzielania osobom, których dane dotyczą, informacji na mocy art. 10 i 11).

Po przeanalizowaniu i porównaniu obu tych stron można ustalić tymczasową „równowagę". W przypadku gdy wynik oceny wciąż pozostawia wątpliwości, następnym krokiem będzie ocenienie, czy dodatkowe gwarancje, dające większą ochronę osobie, której dane dotyczą, mogą przechylić szalę w taki sposób, że przetwarzanie byłoby legalne.

a) Ocena uzasadnionego interesu administratora danych

Podczas gdy pojęcie uzasadnionych interesów jest dość szerokie, jak wyjaśniono w sekcji III.3.1 powyżej, jego charakter odgrywa kluczową rolę, jeśli chodzi o ważenie interesów w stosunku do praw i interesów osób, których dane dotyczą. Chociaż niemożliwe jest sformułowanie wartościującego osądu w odniesieniu do wszystkich możliwych uzasadnionych interesów, możliwe jest przedstawienie pewnych wskazówek. Jak wspomniano powyżej, taki interes może być banalny lub ważny, jasny lub bardziej kontrowersyjny.

(i) Korzystanie z prawa podstawowego

Kilka spośród podstawowych praw i wolności zapisanych w Karcie praw podstawowych Unii Europejskiej („Karta")[70] i europejskiej konwencji praw człowieka („EKPC") może wchodzić w konflikt z prawem do prywatności i prawem do ochrony danych osobowych. Jest to wolność wypowiedzi i informacji[71], wolność sztuk i nauk[72], prawo dostępu do dokumentów[73], a także na przykład prawo do wolności i bezpieczeństwa osobistego[74], wolność myśli, sumienia i religii[75], wolność prowadzenia działalności gospodarczej[76], prawo własności[77],

[69] Ze względu na ich wagę, niektóre konkretne kwestie dotyczące gwarancji zostaną dalej omówione w odrębnych punktach w sekcjach III.3.5 oraz III.3.6.
[70] Postanowienia Karty skierowane są do instytucji i organów UE z należytym uwzględnieniem zasady pomocniczości oraz do krajowych organów wyłącznie wówczas, gdy wdrażają przepisy UE.
[71] Artykuł 11 Karty oraz art. 10 EKPC.
[72] Artykuł 13 Karty oraz art. 9 i 10 EKPC.
[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 instytucji, organów i jednostek organizacyjnych Unii, niezależnie od ich formy". Podobne prawa dostępu istnieją w kilku państwach członkowskich w odniesieniu do dokumentów przechowywanych przez organy publiczne w tych państwach.
[74] Artykuł 6 Karty oraz art. 5 EKPC.
[75] Artykuł 10 Karty oraz art. 9 EKPC.
[76] Artykuł 16 Karty.
[77] Artykuł 17 Karty oraz art. 1 protokołu nr 1 do EKPC.

prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu[78] czy domniemanie niewinności i prawo do obrony[79].

Aby uzasadniony interes administratora danych przeważał, przetwarzanie danych musi być „konieczne" i „proporcjonalne" w celu wykonywania danego prawa podstawowego.

Przykładowo w zależności od okoliczności danego przypadku opublikowanie pewnych obciążających informacji na temat wydatków urzędnika państwowego wysokiego szczebla, który jest zaangażowany w rzekomą aferę korupcyjną, może okazać się konieczne i proporcjonalne dla pewnej gazety. Z drugiej strony, nie powinno być ogólnego przyzwolenia na publikowanie przez media wszelkich nieistotnych szczegółów życia prywatnego osób publicznych. Te i podobne przypadki zazwyczaj wiążą się ze skomplikowanymi kwestiami oceny. Ważną rolę mogą odgrywać szczegółowe przepisy, orzecznictwo, praktyka sądowa, wytyczne oraz kodeksy postępowania i inne formalne lub mniej formalne standardy, które mogą być pomocne w przeprowadzeniu tej oceny[80].

W stosownych przypadkach, również w tym kontekście, dodatkowe gwarancje mogą odgrywać ważną rolę i pomóc określić, w jaki sposób można znaleźć – czasami delikatną – równowagę.

(ii) Interesy publiczne/interesy szerszej społeczności

W niektórych przypadkach administrator danych może chcieć powołać się na interes publiczny lub interes szerszej społeczności (bez względu na to, czy jest to przewidziane w krajowych przepisach ustawowych lub wykonawczych). Na przykład organizacja charytatywna może przetwarzać dane osobowe na potrzeby badań medycznych lub organizacja niekomercyjna może przetwarzać dane w celu podniesienia świadomości w zakresie korupcji w rządzie.

Może być również tak, że prywatny interes biznesowy przedsiębiorstwa pokrywa się w pewnym stopniu z interesem publicznym. Może się tak zdarzyć na przykład w odniesieniu do zwalczania nadużyć finansowych lub innego rodzaju nielegalnego korzystania z usług[81]. Usługodawca może mieć uzasadniony interes biznesowy w zapewnieniu, aby jego klienci nie nadużywali jego usługi (lub nie byli w stanie uzyskać usług bez zapłaty), podczas gdy klienci tego przedsiębiorstwa, podatnicy i ogół społeczeństwa również mają uzasadniony interes w

[78] Artykuł 47 Karty oraz art. 6 EKPC.
[79] Artykuł 48 Karty oraz art. 6 i 13 EKPC.
[80] W odniesieniu do kryteriów, które należy stosować w przypadkach dotyczących wolności wypowiedzi, pomocne wskazówki znajdują się także w orzecznictwie Europejskiego Trybunału Praw Człowieka. Zob. np. wyrok Europejskiego Trybunału Praw Człowieka z dnia 7 lutego 2012 r. w sprawie von Hannover przeciwko Niemcom (nr 2), w szczególności pkt 95–126. Trzeba również wziąć pod uwagę fakt, że art. 9 dyrektywy (zatytułowany *Przetwarzanie danych osobowych i wolność wypowiedzi*) daje państwom członkowskim „możliwość wyłączenia lub odstąpienia od [określonych przepisów dyrektywy] w przypadku przetwarzania danych osobowych wyłącznie w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego", pod warunkiem że jest to „konieczne dla pogodzenia prawa do zachowania prywatności z przepisami dotyczącymi wolności wypowiedzi".
[81] Zob. np. „Przykład 21: Eksploracja danych dotyczących inteligentnego pomiaru zużycia energii w celu wykrywania nieuprawnionego zużycia energii" na s. 67 opinii 3/2013 Grupy Roboczej w sprawie celowości (przywołanej powyżej w przypisie 9).

zapewnieniu zniechęcania do popełniania oszustw i wykrywania takich przestępstw w przypadku ich wystąpienia.

Ogólnie rzecz biorąc, fakt, że administrator danych działa nie tylko we własnym uzasadnionym interesie (np. biznesowym), ale również w interesie szerszej społeczności, może sprawiać, że interes ten ma większą „wagę". Im ważniejszy jest interes publiczny lub interes szerszej społeczności oraz im wyraźniej społeczność i osoby, których dane dotyczą, uznają i oczekują, że administrator danych może podejmować działania i przetwarzać dane na potrzeby realizacji tych interesów, tym większą wagę ma ten uzasadniony interes.

Z drugiej strony, „egzekwowanie prawa na drodze prywatnoprawnej" nie powinno być wykorzystywane do uzasadniania inwazyjnych praktyk, które – gdyby stosowała je organizacja rządowa – byłyby zabronione na podstawie orzecznictwa Europejskiego Trybunału Praw Człowieka ze względu na to, że działania władzy publicznej stanowiłyby ingerencję w prywatność osób, których dane dotyczą, a nie spełniałyby rygorystycznych wymogów na mocy art. 8 ust. 2 EKPC.

(iii) Inne uzasadnione interesy

Jak już omówiono w sekcji III.2, w niektórych przypadkach kontekst, w którym pojawia się uzasadniony interes, może być zbliżony do jednego z kontekstów, w których mogą stosować się pewne inne podstawy prawne, w szczególności podstawy prawne określone w art. 7 lit. b) (umowa), lit. c) (zobowiązanie prawne) lub lit. e) (zadanie publiczne). Na przykład przetwarzanie danych może nie być absolutnie konieczne, lecz wciąż może być istotne dla realizacji umowy – lub przetwarzanie pewnych danych może być jedynie dozwolone w prawie, a nie wymagane. Jak widać, nie zawsze łatwo jest wyznaczyć wyraźną linię podziału między różnymi podstawami, ale właśnie z tego względu tym ważniejsze jest uwzględnienie w analizie testu równowagi na mocy art. 7 lit. f).

Również w tej sytuacji, jak również we wszystkich możliwych innych przypadkach, których dotychczas nie wymieniono, im ważniejszy jest interes administratora danych oraz im wyraźniej szersza społeczność uznaje i oczekuje, że administrator danych może podejmować działania i przetwarzać dane na potrzeby realizacji tego interesu, tym większą wagę ma ten uzasadniony interes[82]. To prowadzi do następnego, bardziej ogólnego punktu.

(iv) Prawne i kulturowe/społeczne uznanie zasadności interesów

We wszystkich powyższych kontekstach z pewnością jest również istotne, czy prawo UE lub prawo państwa członkowskiego wyraźnie umożliwia (nawet jeśli tego nie wymaga) administratorom danych podejmowanie kroków w celu realizacji interesu publicznego lub prywatnego. Istotne jest również istnienie jakichkolwiek należycie przyjętych i niewiążących wytycznych wydanych przez właściwe organy, na przykład przez agencje regulacyjne, w których zachęca się administratorów danych do przetwarzania danych w ramach realizacji danego interesu.

[82] Oczywiście ocena musi również obejmować refleksję nad możliwymi szkodami ponoszonymi przez administratora danych, osoby trzecie lub szerszą społeczność, w przypadku gdy nie dochodzi do przetwarzania danych osobowych.

Zgodność z jakimikolwiek niewiążącymi wytycznymi zapewnionymi przez organy ochrony danych lub inne właściwe organy w odniesieniu do sposobów przetwarzania danych także może przyczynić się do pozytywnej oceny równowagi. Oczekiwania kulturowe i społeczne, nawet jeśli nie są odzwierciedlone bezpośrednio w instrumentach ustawodawczych lub regulacyjnych, również mogą odgrywać rolę i mogą pomóc przechylić szalę na którąś ze stron.

Im wyraźniej uznaje się w przepisach, w innych instrumentach regulacyjnych – wiążących dla administratora danych lub nie – lub nawet w kulturze danej społeczności w ujęciu ogólnym, bez konkretnej podstawy prawnej, że administratorzy danych mogą podejmować działania i przetwarzać dane na potrzeby realizacji określonego interesu, tym większą wagę ma ten uzasadniony interes[83].

b) Wpływ na osoby, których dane dotyczą

Jeżeli chodzi o drugą stronę równowagi, kluczowym kryterium jest wpływ przetwarzania na interesy lub podstawowe prawa i wolności osoby, której dane dotyczą. W pierwszej podsekcji poniżej ogólnie omówiono, jak ocenić wpływ na osobę, której dane dotyczą.

W tym kontekście użytecznych może być szereg elementów, które przeanalizowano w dalszych podsekcjach, w tym charakter danych osobowych, sposób przetwarzania informacji, uzasadnione oczekiwania osób, których dane dotyczą, oraz status administratora danych i osoby, której dane dotyczą. Pokrótce omówione zostaną również kwestie związane z potencjalnymi źródłami ryzyka, które mogą prowadzić do wpływu na zainteresowane osoby, dotkliwość wszelkiego wpływu na zainteresowane osoby i prawdopodobieństwo zaistnienia takiego wpływu.

[83] Interesu tego nie można jednak wykorzystywać do uzasadnienia praktyk inwazyjnych, które w innym wypadku nie przeszłyby testu na mocy art. 8 ust. 2 EKPC.

(i) Ocena wpływu

Przy ocenie wpływu[84] przetwarzania należy wziąć pod uwagę konsekwencje – zarówno pozytywne, jak i negatywne. Mogą one obejmować potencjalne przyszłe decyzje lub działania osób trzecich oraz sytuacje, w których przetwarzanie może prowadzić do wykluczenia lub dyskryminacji osób fizycznych, zniesławienia lub, w szerszym ujęciu, sytuacji, w których występuje ryzyko szkody dla reputacji, pozycji negocjacyjnej lub niezależności osoby, której dane dotyczą.

Oprócz niekorzystnych skutków, które mogą być szczegółowo przewidziane, należy również wziąć pod uwagę szersze skutki emocjonalne, takie jak: irytacja, strach i stres, które mogą być wynikiem utraty przez osobę, której dane dotyczą, kontroli nad danymi osobowymi lub świadomości, że doszło lub że może dojść do wykorzystania niezgodnie z przeznaczeniem lub naruszenia tych danych – na przykład poprzez upublicznienie w Internecie. Należy również należycie uwzględnić hamujący wpływ na chronione zachowania, takie jak wolność prowadzenia badań lub wolność słowa, który może być skutkiem ciągłego monitorowania/śledzenia.

Grupa Robocza podkreśla, że kluczowe jest zrozumienie, że dany „wpływ" jest znacznie szerszym pojęciem niż krzywda lub szkoda dla jednej osoby, której dane dotyczą, lub większej liczby takich osób. „Wpływ" w znaczeniu używanym w niniejszej opinii obejmuje każdą możliwą (potencjalną lub faktyczną) konsekwencję przetwarzania danych. Dla zachowania jasności należy również podkreślić, że pojęcie to nie jest związane z pojęciem naruszenia ochrony danych i jest znacznie szersze niż wpływ, który może być skutkiem naruszenia ochrony danych. Pojęcie wpływu w sensie, w jakim jest ono używane w niniejszej opinii, obejmuje różne sposoby, w jakie przetwarzanie danych osobowych może dotykać – pozytywnie lub negatywnie – osobę, której dane dotyczą[85].

Istotne jest również zrozumienie, że zazwyczaj szereg powiązanych i niepowiązanych wydarzeń może łącznie prowadzić do ostatecznie negatywnego wpływu na osobę, której dane dotyczą, i może być trudno określić, która operacja przetwarzania danych przeprowadzona przez którego administratora danych odegrała kluczową rolę w spowodowaniu tego negatywnego wpływu.

Biorąc pod uwagę, że rozpoczęcie postępowania odszkodowawczego za poniesioną krzywdę lub szkodę jest w tym kontekście często trudne dla osób, których dane dotyczą, nawet jeżeli

[84] Ocenę wpływu należy rozumieć w kontekście artykułu 7 lit. f). Innymi słowy, nie ma odniesienia do „analizy ryzyka" ani „oceny skutków w zakresie ochrony danych" w rozumieniu zawartym w proponowanym rozporządzeniu (art. 33 i 34) i w różnych poprawkach do niego proponowanych przez komisję LIBE. Kwestia tego, jaką metodykę należy stosować przy „analizie ryzyka" czy też „ocenie skutków w zakresie ochrony danych" wykracza poza zakres niniejszej opinii. Z drugiej strony należy pamiętać, że – w ten czy inny sposób – analiza wpływu na mocy art. 7 lit. f) może stanowić istotną część każdej „oceny ryzyka" czy „oceny skutków w zakresie ochrony danych" i może również pomóc określić sytuacje, w których należy konsultować się z organem ochrony danych.

[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 szkody na osobie, bólu, cierpienia i utraty przyjemności, co mogłoby ostatecznie wynikać np. z nieuprawnionej zmiany historii choroby, oraz następującego niewłaściwego leczenia pacjenta, zawsze należy brać odpowiednio pod uwagę, choć w żadnym razie nie jest to ograniczone do sytuacji objętych zakresem stosowania art. 7 lit. f). Jednocześnie takie ryzyko nie jest jedynym zagrożeniem, które należy uwzględnić przy ocenie wpływu na mocy art. 7 lit. f).

sam skutek jest jak najbardziej rzeczywisty, tym ważniejsze jest skupienie się na zapobieganiu oraz zapewnianiu, aby działalność związana z przetwarzaniem danych mogła być prowadzona tylko wtedy, gdy nie niesie ze sobą ryzyka lub stwarza bardzo małe ryzyko nadmiernego negatywnego wpływu na interesy lub podstawowe prawa i wolności osób, których dane dotyczą.

Przy ocenie wpływu terminologia i metodyka tradycyjnej oceny ryzyka mogą być w pewnym stopniu użyteczne, dlatego niektóre elementy tej metodyki zostaną pokrótce omówione poniżej. Całościowa metodyka oceny wpływu – w kontekście art. 7 lit. f) lub szerszym – wykraczałaby jednak poza zakres niniejszej opinii.

W tym kontekście, podobnie jak w innych sytuacjach, istotne jest określenie źródeł potencjalnego wpływu 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 mogą stanowić czułe punkty, które hakerzy mogliby wykorzystać. To źródło ryzyka niesie ze sobą względnie wysokie prawdopodobieństwo, że ryzyko naruszenia ochrony danych się urzeczywistni. Homogeniczny, stabilny system, który nie ma połączeń i jest odłączony od Internetu, niesie natomiast dużo mniejsze prawdopodobieństwo naruszenia ochrony danych.

Innym elementem oceny ryzyka jest powaga konsekwencji urzeczywistnionego ryzyka. Może ona mieć poziom od niskiego (np. irytująca konieczność ponownego podania danych kontaktowych utraconych przez administratora danych) po bardzo wysoki (jak utrata życia, gdy informacje o lokalizacji chronionych osób dostaną się w ręce przestępców lub gdy zasilanie jest zdalnie odcięte poprzez inteligentne urządzenia pomiarowe w przypadku krytycznych warunków pogodowych lub osobistego stanu zdrowia).

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

Na koniec przy stosowaniu metodologii należy pamiętać, że ocenianie wpływu na mocy art. 7 lit. f) nie może prowadzić do mechanicznych oraz czysto ilościowych działań. W tradycyjnych scenariuszach oceny ryzyka powaga może także uwzględniać liczbę osób potencjalnie objętych wpływem. Należy jednak pamiętać, że przetwarzanie danych osobowych mające wpływ na mniejszość osób, których dane dotyczą – lub nawet tylko na jedną osobę – ciągle wymaga bardzo starannej analizy, w szczególności jeżeli taki wpływ na każdą osobę zainteresowaną 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 na mocy 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, zdaniem Grupy Roboczej co do zasady wykorzystanie biometrii do celów ogólnych wymogów bezpieczeństwa własności lub osób fizycznych jest uznawane za uzasadniony interes, wobec którego nadrzędne byłyby 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, pod warunkiem że administrator przedstawił konkretne dowody występowania znaczącego ryzyka[87].

Ogólnie rzecz biorąc, im bardziej wrażliwe są informacje, tym więcej konsekwencji może z tego wyniknąć dla osoby, której dane dotyczą. Nie oznacza to jednak, że dane, które same w sobie mogą wydać się nieszkodliwe, mogą być dowolnie przetwarzane na podstawie art. 7 lit. f). Nawet takie dane, w zależności od sposobu, w jaki są przetwarzane, mogą mieć znaczący wpływ na osoby fizyczne, jak to zostanie pokazane w podsekcji (iii) poniżej.

W tym względzie może mieć znaczenie fakt, czy dane zostały upublicznione przez osobę, której dane dotyczą, czy przez osoby trzecie. Trzeba tu przede wszystkim podkreślić, że dane osobowe, nawet jeżeli zostały upublicznione, ciągle są uważane za dane osobowe, dlatego ich przetwarzanie nadal wymaga odpowiednich gwarancji[88]. Nie ma generalnego pozwolenia na ponowne wykorzystanie oraz dalsze przetwarzanie publicznie dostępnych danych osobowych na mocy art. 7 lit. f).

Okoliczność, że dane osobowe są publicznie dostępne, może być uznana za czynnik w ocenie, zwłaszcza jeżeli publikacja została przeprowadzona w ramach uzasadnionego oczekiwania co do dalszego wykorzystania danych dla pewnych celów (np. dla celów badań naukowych lub dla celów związanych z przejrzystością i rozliczalnością).

(iii) Sposób przetwarzania danych

Ocena wpływu w szerszym znaczeniu może obejmować rozważenie tego, czy dane są podawane do wiadomości publicznej lub w inny sposób udostępniane dużej liczbie osób, lub czy też duże ilości danych osobowych są przetwarzane lub zestawiane z innymi danymi (np. w przypadku profilowania, w celach handlowych, w celach egzekwowania prawa lub w innych celach). Pozornie nieszkodliwe dane, kiedy są przetwarzane na dużą skalę oraz

[86] Dane biometryczne i informacje genetyczne uznawane są za szczególne kategorie danych we wniosku Komisji dotyczącym rozporządzenia o ochronie danych, w związku ze zmianami proponowanymi przez komisję LIBE.. Patrz poprawka 103 do art. 9 w sprawozdaniu końcowym komisji LIBE. W kwestii związku między art. 7 i 8 dyrektywy 95/46/WE zob. sekcja III.1.2 powyżej, s. 16–17.

[87] Zob. opinia 3/2012 Grupy Roboczej Art. 29 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP193). Tytułem innego przykładu, w swojej opinii 4/2009 dotyczącej Światowej Agencji Antydopingowej (przytoczonej powyżej w przypisie 32) Grupa Robocza podkreśliła, że art. 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 art. 8 ust. 4 i 5 dyrektywy.

[88] Zob. opinia 3/2013 Grupy Roboczej w sprawie celowości (przywołana w przypisie 9 powyżej) oraz opinia 6/2013 Grupy Roboczej w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (ISP) , przyjęta 05.06.2013 r. (WP 207).

zestawiane z innymi danymi, mogą prowadzić do wyciągnięcia wniosków na temat danych szczególnie chronionych, jak pokazano powyżej w scenariuszu 3, ilustrującym związek między wzorcami konsumpcji pizzy a składkami na ubezpieczenie zdrowotne.

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

W poprzedniej opinii Grupa Robocza zwróciła uwagę także na ryzyko nierozerwalnie związane z określonymi rozwiązaniami w dziedzinie bezpieczeństwa (włączając w to zapory sieciowe, antywirusowe lub antyspamowe), gdyż może ono prowadzić do zastosowania głębokiej inspekcji pakietów na dużą skalę, co może mieć znaczący wpływ na ocenę równowagi praw[90].

Ogólnie rzecz biorąc, im bardziej negatywny lub niepewny może być wpływ przetwarzania, tym mniej prawdopodobne jest to, że przetwarzanie będzie w zasadzie uznane za uzasadnione. Dostępność alternatywnych metod osiągnięcia celów administratora danych, wywierających mniej negatywny wpływ na osobę, której dane dotyczą, byłaby z pewnością istotnym czynnikiem w tym kontekście. W stosownych przypadkach można wykorzystać oceny skutków w zakresie ochrony danych i prywatności, aby ustalić, czy istnieje taka możliwość.

(iv) Uzasadnione oczekiwania osoby, której dane dotyczą

Uzasadnione oczekiwania osoby, której dane dotyczą, w odniesieniu do wykorzystania oraz ujawniania danych również są bardzo istotne pod tym względem. Jak również podkreślono w odniesieniu do analizy zasady celowości[91], jest „ważne, aby rozważyć, czy status administratora danych[92], charakter związku lub dostarczone usługi[93] bądź mające zastosowanie zobowiązania prawne lub umowne (lub inne obietnice poczynione w momencie gromadzenia danych) mogą dać początek uzasadnionym oczekiwaniom co do ściślejszej poufności oraz ściślejszego ograniczenia dalszego wykorzystania. Ogólnie rzecz biorąc, im bardziej szczegółowy i restrykcyjny jest kontekst gromadzenia danych, tym bardziej prawdopodobne, że będzie więcej ograniczeń wykorzystania tych danych. Również w tym przypadku konieczne jest uwzględnienie raczej rzeczywistego kontekstu niż po prostu opieranie się na tekście napisanym drobnym drukiem.

(v) Status administratora danych oraz osoby, której dane dotyczą

Status osoby, której dane dotyczą, i administratora danych jest również istotny przy ocenie wpływu przetwarzania. W zależności od tego, czy administrator danych jest osobą fizyczną,

[89] Zob. sekcja III.2.5 oraz załącznik 2 (Duże zbiory danych i otwarte dane) do opinii w sprawie celowości (przytoczonej powyżej w przypisie 9).
[90] Zob. sekcja 3.1 opinii 1/2009 Grupy Roboczej w sprawie wniosków zmieniających dyrektywę 2002/58/WE o prywatności i łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (WP159).
[91] Zob. s. 24–25 opinii 3/2013 Grupy Roboczej w sprawie celowości (przywołanej w przypisie 9 powyżej).
[92] „Np. adwokat lub lekarz".
[93] „Np. usługi przetwarzania w chmurze do zarządzania dokumentami osobistymi, usługi poczty elektronicznej, kalendarze, e-czytniki wyposażone w funkcję robienia notatek oraz różne aplikacje do tzw. life-loggingu, które mogą zawierać dane osobowe".

małą organizacją, dużym przedsiębiorstwem wielonarodowym czy organem sektora publicznego, oraz od konkretnych okoliczności jego pozycja może być bardziej lub mniej dominująca w odniesieniu do osoby, której dane dotyczą. Duże przedsiębiorstwo wielonarodowe 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 narzucenia tej osobie tego, co uznaje za swój „uzasadniony interes". Tym bardziej może tak być, jeżeli przedsiębiorstwo ma pozycję dominującą na rynku. Jeżeli kwestia ta pozostanie niesprawdzona, może dziać się to ze szkodą dla poszczególnych osób, których dane dotyczą. Podobnie jak przepisy o ochronie konsumentów i konkurencji pomagają zapewnić, aby pozycja ta nie została wykorzystana w niewłaściwy sposób, przepisy o ochronie danych również mogą odgrywać znaczącą rolę w zapewnianiu, aby prawa i interesy osób, których dane dotyczą, nie były nadmiernie naruszane.

Z drugiej strony status osoby, której dane dotyczą, jest również istotny. Podczas gdy co do zasady test równowagi powinien odnosić się do przeciętnej osoby fizycznej, konkretne sytuacje powinny prowadzić do podejścia opartego na poszczególnych przypadkach: na przykład właściwe byłoby rozważenie, czy osoba, której dane dotyczą, jest dzieckiem[94] lub pod innym względem należy do grupy ludności wymagającej szczególnego traktowania, jak np. chorzy umysłowo, osoby ubiegające się o azyl czy osoby starsze. To, czy osoba, której dane dotyczą, jest pracownikiem, studentem, pacjentem lub czy w jakiś inny sposób istnieje nierównowaga pomiędzy pozycją osoby, której dane dotyczą, a pozycją administratora, musi także z pewnością być istotne. Ważne jest, aby ocenić efekt faktycznego przetwarzania dla poszczególnych osób fizycznych.

Na koniec trzeba podkreślić, że nie każdy negatywny wpływ na osoby, których dane dotyczą, ma taką samą wagę. Celem testu równowagi na mocy art. 7 lit. f) nie jest zapobieżenie jakiemukolwiek negatywnemu wpływowi na osobę, której dane dotyczą. Jego celem jest raczej zapobieżenie nieproporcjonalnemu wpływowi. Jest to zasadnicza różnica. Na przykład publikacja dobrze udokumentowanego i dokładnego artykułu prasowego na temat rzekomej korupcji rządu może spowodować szkody dla urzędników, których ten artykuł dotyczy, oraz może prowadzić do znaczących konsekwencji, włączając w to utratę reputacji, utratę wyborców lub pozbawienie wolności, jednak wciąż jej podstawę mógłby stanowić art. 7 lit. f)[95].

c) Tymczasowa równowaga

Przy wyważaniu przedmiotowych 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, aby administrator danych spełniał wymogi art. 7 lit. f). Pełna zgodność powinna oznaczać, że wpływ na osoby fizyczne jest ograniczony, że istnieje *mniejsze prawdopodobieństwo*, że interesy lub prawa i wolności osób, których dane dotyczą, zostaną naruszone, oraz że dlatego jest *bardziej prawdopodobne*, że administrator

[94] Zob. opinia 2/2009 Grupy Roboczej Art. 29 w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół), przyjęta w dniu 11.02.2009 r. (WP160). W opinii tej kładzie się nacisk na szczególną wrażliwość dziecka, a w przypadku, gdy dziecko jest reprezentowane, na potrzebę wzięcia pod uwagę dobra dziecka, a nie interesu jego przedstawiciela.

[95] Jak wyjaśniono powyżej, należy również wziąć pod uwagę wszelkie istotne wyłączenia dotyczące przetwarzania do celów dziennikarskich na mocy art. 9 dyrektywy.

danych może oprzeć się na art. 7 lit. f). Powinno to zachęcić administratorów danych do lepszego przestrzegania wszystkich przepisów horyzontalnych 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). Co więcej, w takiej sytuacji art. 7 lit. f) byłby zbędny lub stałby się luką w prawie, która sprawiłaby, że cały art. 7, który zawiera wymóg przedstawienia odpowiedniej, konkretnej podstawy prawnej dla przetwarzania, straciłby znaczenie.

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

Dodatkowe środki mogą obejmować na przykład zapewnienie sprawnego, łatwego w obsłudze i dostępnego mechanizmu, który daje osobom, których dane dotyczą, bezwarunkową możliwość zrezygnowania z przetwarzania. Te dodatkowe środki mogą w niektórych (ale nie we wszystkich) przypadkach pomóc przechylić szalę oraz pomóc zapewnić, aby przetwarzanie mogło być oparte na art. 7 lit. f), jednocześnie chroniąc prawa i interesy osób, których dane dotyczą.

(d) Dodatkowe gwarancje stosowane przez administratora danych

Jak to wyjaśniono powyżej, sposób, w jaki administrator zastosowałby odpowiednie środki, może w niektórych sytuacjach pomóc „przechylić szalę" wagi. To, czy wynik jest akceptowalny, będzie zależało od całej oceny. Im istotniejszy jest wpływ na osobę, której dane dotyczą, tym większą uwagę należy zwrócić na odpowiednie gwarancje.

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

W niektórych innych przypadkach gwarancje nie są *wyraźnie* wymagane w dyrektywie, ale mogą być w przyszłości wymagane na mocy proponowanego rozporządzenia, lub są one wymagane tylko w konkretnych sytuacjach, na przykład:

- środki techniczne i organizacyjne mające na celu zapewnienie, aby nie można było wykorzystać danych do podejmowania decyzji lub innych działań w stosunku do osób fizycznych („rozdział funkcjonalny", częsty w kontekście badań naukowych);
- szerokie wykorzystanie technik anonimizacji;

[96] W kwestii ważnej roli „zgodności horyzontalnej" zob. również s. 54 opinii 3/2013 Grupy Roboczej w sprawie celowości, przywołanej w przypisie 9 powyżej.

- agregacja danych;
- technologie służące wzmocnieniu ochrony prywatności, uwzględnienie ochrony prywatności już w fazie projektowania, oceny skutków w zakresie ochrony danych i prywatności;
- większa przejrzystość;
- ogólne i bezwarunkowe prawo do rezygnacji;
- możliwość przenoszenia danych oraz powiązane środki służące wzmocnieniu pozycji osób, których dane dotyczą.

Grupa Robocza zwraca uwagę, że w odniesieniu do niektórych kluczowych kwestii, obejmujących rozdział funkcjonalny i techniki anonimizacji, pewne wytyczne zostały już przedstawione w odpowiednich częściach jej opinii w sprawie celowości, w sprawie otwartych danych data oraz w sprawie technik anonimizacji[97].

Jeżeli chodzi o techniki pseudonimizacji 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 czynnik zmieniający nielegalne przetwarzanie w legalne[98].

Jednocześnie pseudonimizacja i szyfrowanie, podobnie jak wszystkie inne techniczne i organizacyjne środki wprowadzone w celu ochrony danych 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 szali na stronę administratora danych. Wykorzystanie mniej ryzykownych form przetwarzania danych osobowych (np. danych osobowych, które są szyfrowane podczas przechowywania czy transmisji, lub danych osobowych, które są mniej bezpośrednio i w mniej łatwy sposób możliwe do zidentyfikowania), powinno na ogół oznaczać, że prawdopodobieństwo ingerencji w interesy lub podstawowe prawa i wolności osób, których dane dotyczą, jest zmniejszone.

W związku z tymi gwarancjami – 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 sprzeciwu osoby, której dane dotyczą, wobec przetwarzania oraz, poza sprzeciwem, dostępność mechanizmu rezygnacji bez konieczności uzasadnienia, oraz
- wzmocnienie pozycji osób, których dane dotyczą: możliwość przenoszenia danych oraz dostępność sprawnych mechanizmów umożliwiających osobie, której dane dotyczą, dostęp do jej danych, ich zmienianie, usuwanie, przenoszenie lub dalsze

[97] Zob. sekcje III.2.3 i III.2.5 opinii 3/2013 Grupy Roboczej w sprawie celowości, przywołanej w przypisie 9 powyżej, oraz załącznik 2 do tej opinii, w kwestii dalszego przetwarzania do celów historycznych, statycznych i naukowych oraz dużych zbiorów danych i otwartych danych; zob. również odpowiednie fragmenty opinii 6/2013 Grupy Roboczej w sprawie otwartych danych (przywołanej w przypisie 88 powyżej) oraz opinii 5/2014 w sprawie technik anonimizacji.

[98] W tej kwestii zob. poprawki przegłosowane przez komisję LIBE w sprawozdaniu końcowym komisji LIBE, a w szczególności poprawka 15 w motywie 38 łącząca pseudonimizację i uzasadnione oczekiwania osoby, której dane dotyczą.

przetwarzanie w inny sposób (lub umożliwiających dalsze przetwarzanie osobom trzecim).

Ze względu na ich istotność tematy te zostaną przedyskutowane w oddzielnych punktach.

III.3.5. Rozliczalność i przejrzystość

W pierwszej kolejności, zanim rozpocznie się operacja przetwarzania na podstawie art. 7 lit. f), administrator danych ma obowiązek ocenić, czy ma uzasadniony interes, czy przetwarzanie jest konieczne dla tego prawnie uzasadnionego interesu oraz czy w konkretnym przypadku interesy i prawa osób, których dane dotyczą, są nadrzędne wobec tego interesu.

W tym sensie art. 7 lit. f) jest oparty na zasadzie rozliczalności. Administrator danych musi przeprowadzić dokładny i skuteczny test zawczasu, opierając się raczej na konkretnych okolicznościach danego przypadku niż na abstrakcyjnych założeniach i biorąc pod uwagę uzasadnione oczekiwania osób, których dane dotyczą. W ramach dobrej praktyki w stosownych przypadkach przeprowadzenie testu powinno być udokumentowane w wystarczająco szczegółowy i przejrzysty sposób, tak aby pełne i poprawne zastosowanie testu mogło być zweryfikowane – w razie konieczności – przez odpowiednie zainteresowane osoby, włączając w to osoby, których dane dotyczą, oraz organy ochrony danych i ostatecznie sądy.

Administrator danych w pierwszej kolejności określa uzasadniony interes oraz przeprowadza test równowagi, jednak niekoniecznie jest to ostateczna definitywna ocena: jeżeli w rzeczywistości interes realizowany przez administratora danych nie jest tym, który administrator określił, lub jeżeli administrator zdefiniował interes w niewystarczająco szczegółowy sposób, równowagę trzeba ponownie ocenić w oparciu o rzeczywisty interes, który określa organ ochrony danych albo sąd[99]. Podobnie jak w przypadku innych kluczowych aspektów ochrony danych, takich jak identyfikacja administratora danych czy określenie celu[100], liczą się realia, a nie twierdzenia administratora danych.

Pojęcie rozliczalności jest ściśle powiązane z pojęciem przejrzystości. W celu umożliwienia osobom, których dane dotyczą, wykonania swoich praw oraz umożliwienia zainteresowanym osobom sprawowania kontroli publicznej w szerszym ujęciu, Grupa Robocza zaleca, żeby administratorzy danych wyjaśnili osobom, których dane dotyczą, w prosty i przyjazny dla użytkownika sposób powody, dla których są oni zdania, że interesy oraz podstawowe prawa i wolności osób, których dane dotyczą, nie są nadrzędne wobec interesów administratorów danych, a także wyjaśnili im gwarancje wprowadzone w celu ochrony danych, w tym w stosownych przypadkach prawo rezygnacji z przetwarzania[101].

---

[99] Np. w związku ze skargą lub sprzeciwem na mocy art. 14.

[100] Zob. opinie przywołane w przypisie 9.

[101] Jak wyjaśniono na s. 46 opinii 3/2013 Grupy Roboczej w sprawie celowości (przywołanej w przypisie 9 powyżej), w przypadku profilowania oraz zautomatyzowanego podejmowania decyzji „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 utworzenia profilu. Innymi słowy, organizacje powinny ujawnić informacje na temat ich kryteriów decyzyjnych. Jest to kluczowa gwarancja i tym bardziej ważna w świecie dużych zbiorów danych". Niezwykle istotnym czynnikiem, który również należy uwzględnić w przypadku wyważania, jest fakt, czy organizacja oferuje taką przejrzystość czy też nie.

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

Jeżeli administrator danych ukrywa ważne informacje dotyczące nieoczekiwanego dalszego wykorzystania danych, stosując prawnicze terminy ujęte drobnym drukiem w umowie, może to naruszać zasady ochrony konsumentów dotyczące nieuczciwych warunków umownych (w tym zakaz „zaskakujących warunków") oraz spowoduje to również niespełnienie wymogów art. 7 lit. a) w odniesieniu do ważnej świadomej zgody lub wymogów art. 7 lit. f) w odniesieniu do uzasadnionych oczekiwań osoby, której dane dotyczą, oraz ogólnej dopuszczalnej równowagi interesów. Oczywiście wzbudziłoby to także wątpliwości dotyczące zgodności z art. 6, jeśli chodzi o potrzebę rzetelnego i legalnego 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 rejestrowane i analizowane w celu wygenerowania wartości dla usługodawców, i dlatego pozostają obojętni na związane z tym ryzyko.

W celu wzmocnienia w tych sytuacjach pozycji osób, których dane dotyczą, pierwszym koniecznym – ale w żadnym razie nie wystarczającym samodzielnie – warunkiem wstępnym[102] jest wyjaśnienie, że usługi nie są darmowe, a raczej że użytkownicy płacą za nie własnymi danymi osobowymi. Warunki i gwarancje, z zastrzeżeniem których dane mogą być wykorzystywane, muszą być jasno przedstawione w każdym przypadku, tak aby zapewnić ważność zgody na mocy art. 7 lit. a) lub korzystną równowagę na mocy art. 7 lit. f).

III.3.6. Prawo sprzeciwu oraz dalsze czynniki

a) Prawo sprzeciwu na mocy art. 14 dyrektywy

Przepisy art. 7 lit. e) i f) mają szczególny charakter w tym sensie, że podczas gdy opierają się one głównie na obiektywnej ocenie przedmiotowych praw i interesów, umożliwiają również uwzględnienie woli osoby, której dane dotyczą, poprzez zapewnienie jej prawa sprzeciwu[103]: przynajmniej w przypadku tych dwóch podstaw art. 14 lit. a) dyrektywy stanowi, że („z zastrzeżeniem odmiennych postanowień ustawodawstwa krajowego") osoba, której dane dotyczą, ma prawo „w dowolnym czasie z ważnych i uzasadnionych przyczyn wynikających z jego konkretnej sytuacji, sprzeciwu co do przetwarzania dotyczących jej danych". W przepisie tym dodano, że jeśli sprzeciw jest uzasadniony, trzeba zaprzestać przetwarzania tych danych.

[102] W kwestii dalszych możliwych gwarancji w odniesieniu do coraz powszechniejszych sytuacji, w których konsumenci płacą swoimi danymi osobowymi, zob. sekcja III.3.6, w szczególności s. 53–54, „Przyjazne dla ochrony danych rozwiązania alternatywne w stosunku do »bezpłatnych« usług internetowych" oraz „Możliwość przenoszenia danych, »midata« oraz powiązane kwestie".

[103] To prawo sprzeciwu nie powinno być mylone ze zgodą w oparciu o art. 7 lit. a), gdzie administrator danych nie może przetwarzać danych przed uzyskaniem takiej zgody. W kontekście art. 7 lit. f) administrator danych może przetwarzać dane, z zastrzeżeniem warunków i gwarancji, o ile osoba, której dane dotyczą, nie wyraziła sprzeciwu. W tym rozumieniu prawo sprzeciwu można raczej uznać za specjalną formę rezygnacji z przetwarzania. Zob. więcej szczegółów w opinii 15/2011 Grupy Roboczej w sprawie definicji zgody (przywołanej w przypisie 2).

Zgodnie z obowiązującym prawem osoba, której dane dotyczą, będzie musiała więc z zasady wykazać „ważne uzasadnione interesy", aby zatrzymać przetwarzanie jej danych osobowych (art. 14 lit. a)), chyba że ma to miejsce w kontekście marketingu bezpośredniego, w którym to przypadku sprzeciw nie musi być uzasadniony (art. 14 lit. b)).

Nie należy tego postrzegać jako sprzecznego z testem równowagi na mocy art. 7 lit. f), który jest przeprowadzany *a priori*: to raczej uzupełnienie równowagi w tym sensie, że w przypadku gdy przetwarzanie jest dozwolone w oparciu o racjonalną i obiektywną ocenę różnych przedmiotowych praw i interesów, osoba, której dane dotyczą, ma jeszcze *dodatkową* możliwość sprzeciwu z przyczyn odnoszących się do jej szczególnej sytuacji. To następnie będzie musiało prowadzić do nowej oceny z uwzględnieniem konkretnych argumentów przedstawionych przez osobę, której dane dotyczą. Ta nowa ocena z zasady ponownie podlega weryfikacji przez organ ochrony danych lub sądy.

b) Dalsze czynniki poza sprzeciwem: rola rezygnacji jako dodatkowej gwarancji

Grupa Robocza podkreśla, że nawet jeśli prawo sprzeciwu na mocy art. 14 lit. a) wymaga uzasadnienia przez osobę, której dane dotyczą, nie ma przeszkód, żeby administrator danych oferował możliwość rezygnacji, która byłaby szersza, a która nie wymagałaby od osoby, której dane dotyczą, żadnego dodatkowego wykazywania uzasadnionego interesu (ważnego lub nie). Takie bezwarunkowe prawo nie musiałoby być oparte na konkretnej sytuacji osób, których dane dotyczą.

Co więcej, w szczególności w przypadkach granicznych, w których trudno osiągnąć równowagę, dobrze zaprojektowany i sprawny mechanizm rezygnacji, chociaż niekoniecznie zapewniałby osobom, których dane dotyczą, wszystkie elementy, które spełniałyby warunek ważnej zgody na mocy art. 7 lit. a), mógłby odgrywać ważną rolę w ochronie praw i interesów osób, których dane dotyczą.

Wymaga to zróżnicowanego podejścia, w ramach którego rozróżnia się przypadki, w których potrzebna jest zgoda na przetwarzanie na mocy art. 7 lit. a), i przypadki, w których realna możliwość rezygnacji z przetwarzania (w połączeniu z ewentualnymi innymi dodatkowymi środkami) może przyczynić się do ochrony osób, których dane dotyczą, na mocy art. 7 lit. f).

Im szersze zastosowanie ma mechanizm rezygnacji i im łatwiej z niego korzystać, tym bardziej przyczyni się do przechylenia szali na korzyść przetwarzania, żeby znaleźć podstawę prawną w art. 7 lit. f).

Przykład: ewolucja podejścia do marketingu bezpośredniego

Aby pokazać, jak dokonuje się rozróżnienia między przypadkami, w których wymagana jest zgoda na mocy art. 7 lit. a), a przypadkami, w których rezygnacja może być wykorzystana jako gwarancja na mocy art. 7 lit. f), warto posłużyć się przykładem marketingu bezpośredniego, w odniesieniu do którego art. 14 lit. b) dyrektywy tradycyjnie zawiera szczegółowy przepis dotyczący rezygnacji. Aby uwzględnić nowe osiągnięcia

technologiczne, przepis ten został później uzupełniony przepisami szczegółowymi zawartymi w dyrektywie o prywatności i łączności elektronicznej[104].

Na mocy art. 13 dyrektywy o prywatności i łączności elektronicznej w odniesieniu do niektórych rodzajów – bardziej inwazyjnych – działań w zakresie marketingu bezpośredniego (takich jak poczta elektroniczna do celów marketingu bezpośredniego oraz automatyczne urządzenia wywołujące) zgoda jest z reguły wymagana. W drodze wyjątku w przypadku istniejących relacji z klientami, w ramach których administrator danych reklamuje własne „podobne" produkty lub usługi, wystarczy zapewnienie (bezwarunkowej) możliwości rezygnacji bez uzasadnienia.

Technologie ewoluowały, co wymagało podobnych, stosunkowo prostych rozwiązań opartych na podobnej logice na potrzeby nowych praktyk marketingowych.

Po pierwsze, ewoluował sposób dostarczania materiałów marketingowych: zamiast zwykłych wiadomości e-mail przychodzących do skrzynek pocztowych ukierunkowane reklamy behawioralne pojawiają się obecnie również na smartfonach i ekranach komputerów. W niedalekiej przyszłości reklama może być także wbudowana w inteligentne obiekty połączone w internecie przedmiotów.

Po drugie, reklamy stają się coraz bardziej konkretnie ukierunkowane: zamiast opierać się na zwykłych profilach klientów, w coraz większym stopniu monitoruje się działania konsumentów online i offline, gromadzi się dane na ten temat i analizuje je przy użyciu bardziej zaawansowanych zautomatyzowanych metod[105].

W wyniku tych zmian zmienił się cel testu równowagi: kwestią nie jest już prawo do wolności słowa w handlu, ale przede wszystkim interesy gospodarcze organizacji przedsiębiorstw 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 fizycznych oraz ich interesu, aby nie być nadmiernie monitorowanymi.

Ta zmiana w dominujących modelach biznesowych oraz wzrost wartości danych osobowych jako składnika aktywów organizacji przedsiębiorstw wyjaśnia niedawno wprowadzone wymogi uzyskania zgody w tym kontekście na podstawie art. 5 ust. 3 oraz art. 13 dyrektywy o prywatności i łączności elektronicznej.

Istnieją więc różne konkretne reguły, w zależności od formy marketingu, obejmujące:

- bezwarunkowe prawo sprzeciwu wobec marketingu bezpośredniego (przeznaczone dla kontekstu tradycyjnych wiadomości pocztowych oraz dla marketingu podobnych produktów) na mocy art. 14 lit. b) dyrektywy; art. 7 lit. f) mógłby być podstawą prawną w tym przypadku;
- wymóg zgody na mocy art. 13 dyrektywy o prywatności i łączności elektronicznej w odniesieniu do automatycznych urządzeń wywołujących, faksu, wiadomości

[104] W kwestii art. 13 dyrektywy o prywatności i łączności elektronicznej zob. również sekcja III.2.4 opinii 3/2013 Grupy Roboczej w sprawie celowości (przywołanej w przypisie 9 powyżej).
[105] Zob. sekcja III.2.5 oraz załącznik 2 (Duże zbiory danych i otwarte dane) do opinii 3/2013 Grupy Roboczej w sprawie celowości (przytoczonej powyżej w przypisie 9).

tekstowych oraz marketingu wykorzystującego pocztę elektroniczną (z zastrzeżeniem wyłączeń)[106], oraz faktycznie art. 7 lit. a) dyrektywy o ochronie danych;
- wymóg zgody na mocy 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej (oraz art. 7 lit. a) dyrektywy o ochronie danych) w odniesieniu do reklamy behawioralnej opartej na technikach śledzenia, takich jak pliki cookie przechowujące informacje w terminalu użytkownika[107].

Podczas gdy 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 byłyby wytyczne co do tego, w jakich sytuacjach wymagana jest zgoda, o której mowa w art. 7 lit. a), oraz dla których sytuacji osiągnięta jest równowaga na mocy art. 7 lit. f), włączając w to możliwość rezygnacji.

W tym aspekcie użyteczne jest przywołanie opinii Grupy Roboczej w sprawie celowości, gdzie wprost stwierdzono, że „kiedy organizacja chce konkretnie przeanalizować lub przewidzieć osobiste preferencje, zachowania oraz postawy poszczególnych klientów, co następnie dostarczy informacji na potrzeby »środków i decyzji«, które są podejmowane wobec tych klientów… dobrowolna, konkretna, świadoma oraz jednoznaczna zgoda na przetwarzanie prawie zawsze byłaby wymagana, inaczej dalsze wykorzystywanie danych nie zostałoby uznane za zgodne z przepisami. Co ważne, zgoda taka powinna być wymagana na przykład dla celów śledzenia i profilowania na potrzeby marketingu bezpośredniego, reklamy behawioralnej, pośrednictwa w handlu danymi, reklamy opartej na lokalizacji lub badań rynku elektronicznego opartych na śledzeniu”[108].

Przyjazne dla ochrony danych 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 ustalenia, że konsument ma rzeczywiste prawo wyboru, i zatem udzielono ważnej zgody na mocy art. 7 lit. a) – jeżeli administrator danych zaoferował także alternatywną wersję swoich usług, w której „dane osobowe” nie były wykorzystane dla celów marketingowych.

Dopóki takie alternatywne usługi nie będą dostępne, trudniejsze będzie argumentowanie, że ważna (dobrowolna) zgoda została udzielona na mocy art. 7 lit. a) poprzez sam fakt korzystania z bezpłatnych usług lub że równowaga na mocy art. 7 lit. f) powinna być ustalona na korzyść administratora danych.

Powyższe względy uwydatniają ważną rolę, jaką dodatkowe gwarancje, w tym sprawny mechanizm rezygnacji z przetwarzania, mogą odgrywać w zmianie tymczasowej równowagi. Jednocześnie sugerują również, że w niektórych przypadkach art. 7 lit. f) nie może być

[106] Zob. także art. 13 ust. 3 dyrektywy o prywatności i łączności elektronicznej, który to przepis pozostawia państwom członkowskim wybór między mechanizmem wyrażenia zgody a mechanizmem rezygnacji w przypadku marketingu bezpośredniego prowadzonego za pomocą innych środków.
[107] W kwestii stosowania tego przepisu zob. opinia 2/2010 Grupy Roboczej w sprawie internetowej reklamy behawioralnej (WP 171).
[108] Zob. załącznik II (Duże zbiory danych i otwarte dane) do opinii w sprawie celowości (przytoczonej powyżej w przypisie 9), s. 45.

podstawą przetwarzania, a administratorzy danych muszą zapewnić ważną zgodę na mocy art. 7 lit. a) – lub spełnić pewne inne warunki dyrektywy – żeby przetwarzanie miało miejsce.

Możliwość przenoszenia danych, „midata" oraz powiązane kwestie

Wśród dodatkowych gwarancji, które mogą pomóc przechylić szalę, szczególną uwagę należy poświęcić możliwości przenoszenia danych oraz powiązanym środkom, które mogą być coraz bardziej istotne w środowisku internetowym. Grupa Robocza przywołuje swoją opinię w sprawie celowości, w której podkreśliła, że „w wielu sytuacjach gwarancje, np. te pozwalające osobom, których dane dotyczą/klientom na posiadanie bezpośredniego dostępu do swoich danych w formacie przenośnym, przyjaznym dla użytkownika oraz nadającym się do przetwarzania automatycznego, może pomóc poprawić ich pozycję oraz zaradzić gospodarczej nierównowadze pomiędzy dużymi korporacjami z jednej strony, a osobami, których dane dotyczą/konsumentami z drugiej. Pozwoliłoby to także osobom „korzystać z dobrobytu" generowanego przez duże zbiory danych oraz stanowiłoby bodziec dla twórców oprogramowania, aby oferowali dodatkowe opcje i aplikacje swoim użytkownikom[109].

Dostępność sprawnych mechanizmów umożliwiających osobom, których dane dotyczą, dostępu do własnych danych, ich modyfikowanie, usuwanie, przekazywanie lub dalsze przetwarzanie w inny sposób (lub pozwolenia osobom trzecim na dalsze przetwarzanie) wzmocni pozycję osób, których dane dotyczą, oraz pozwoli im czerpać większe korzyści z usług cyfrowych. Dodatkowo może sprzyjać rozwojowi bardziej konkurencyjnego rynku poprzez umożliwienie klientom łatwiejszej zmiany dostawców (np. w kontekście bankowości internetowej lub w przypadku dostawców energii elektrycznej w środowisku inteligentnych sieci energetycznych). W końcu może się także przyczynić do tworzenia dodatkowych usług dodanych przez osoby trzecie, które mogą mieć dostęp do danych klientów na żądanie oraz w oparciu o zgodę klientów. Z tej perspektywy możliwość przenoszenia danych jest dobra nie tylko dla ochrony danych, ale również dla konkurencji oraz ochrony konsumentów[110].

IV. Uwagi końcowe

W niniejszej opinii Grupy Roboczej przeanalizowano kryteria legalności przetwarzania danych określone w art. 7 dyrektywy. Oprócz zapewnienia wskazówek dotyczących praktycznej interpretacji i stosowania art. 7 lit. f) w obowiązujących ramach prawnych opinia ta ma na celu sformułowanie zaleceń dotyczących polityki, aby pomóc osobom odpowiedzialnym za wyznaczanie kierunków polityki w danym obszarze w analizowaniu zmian w obecnych ramach prawnych w zakresie ochrony danych. Przed przedstawieniem tych zaleceń poniżej podsumowano główne ustalenia dotyczące wykładni art. 7.

[109] „Zob. inicjatywy takie jak »midata« w Wielkiej Brytanii, 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 dużych zbiorów danych poprzez posiadanie dostępu do swoich własnych informacji, co umożliwi im podejmowanie lepszych wyborów. Zob. także inicjatywy »Green button« (»Zielony przycisk«), które dają konsumentom dostęp do informacji na temat ich własnego zużycia energii". Więcej informacji na temat inicjatyw w Wielkiej Brytanii i Francji zob.http://www.midatalab.org.uk/ orazhttp://mesinfos.fing.org/

[110] Prawo do możliwości przenoszenia danych – zob. art. 18 proponowanego rozporządzenia.

IV.1. Wnioski

Przegląd art. 7

W art. 7 wymaga się, żeby dane osobowe były przetwarzane tylko wówczas, gdy ma zastosowanie co najmniej jedna z sześciu podstaw prawnych wymienionych w tym artykule.

Pierwsza podstawa, art. 7 lit. a), dotyczy przede wszystkim zgody osoby, której dane dotyczą, jako podstawy legalności. Pozostałe podstawy natomiast umożliwiają przetwarzanie – z zastrzeżeniem gwarancji – w sytuacjach, w których przetwarzanie danych w określonym kontekście w celu zrealizowania określonego uzasadnionego interesu jest – niezależnie od zgody – właściwe i konieczne.

W lit. b), c), d) i e) określono konkretne konteksty, w których przetwarzanie danych osobowych można uznać za legalne. Warunki, które mają zastosowanie w każdym z tych różnych kontekstów, wymagają szczególnej uwagi, ponieważ określają one zakres różnych podstaw legalności. Konkretniej, kryteria „konieczne dla realizacji umowy", „konieczne dla wykonania zobowiązania prawnego", „konieczne dla ochrony żywotnych interesów osób, których dane dotyczą" oraz „konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej" obejmują różne wymogi, które omówiono w sekcji III.2.

Przepis zawarty w lit. f) dotyczy, w ujęciu bardziej ogólnym, (wszelkiego rodzaju) uzasadnionego interesu administratora danych (w dowolnym kontekście). Ten ogólny przepis jest jednak obwarowany wymogiem przeprowadzenia dodatkowego testu równowagi, w którym porównuje się uzasadnione interesy administratora danych – lub osoby trzeciej, lub osób, którym dane są ujawniane – z interesami lub prawami podstawowymi osób, których dane dotyczą.

Rola art. 7 lit. f)

Artykułu 7 lit. f) nie należy postrzegać jako podstawy prawnej, z której można korzystać wyłącznie z umiarem, oraz ostateczności na wypadek rzadkich i nieprzewidzianych sytuacji lub jako ostatniej szansy, w przypadku gdy inne podstawy nie mogą mieć zastosowania. Nie należy jej również postrzegać jako preferowanego rozwiązania ani bezpodstawnie rozszerzać jej stosowania, ponieważ podstawa ta byłaby uważana za mniej ograniczającą niż inne podstawy. Jest raczej tak ważnym środkiem, jak każda z pozostałych podstaw legalności przetwarzania danych osobowych.

Odpowiednie stosowanie art. 7 lit. f) w odpowiednich okolicznościach i z zastrzeżeniem odpowiednich gwarancji może pomóc zapobiegać nieprawidłowemu korzystaniu z innych podstaw prawnych lub nadmiernemu poleganiu na tych innych podstawach. Odpowiednia ocena równowagi na mocy art. 7 lit. f), często wraz z możliwością rezygnacji z przetwarzania, w niektórych przypadkach może być uzasadnioną alternatywą dla niewłaściwego wykorzystania podstawy dotyczącej na przykład „zgody" lub „konieczności realizacji umowy". Rozpatrywany w ten sposób art. 7 lit. f) stanowi uzupełniającą gwarancję w porównaniu z innymi wcześniej ustalonymi podstawami. Nie powinien zatem być traktowany jako „najsłabsze ogniwo" czy furtka legitymizująca wszelką działalność związaną z przetwarzaniem danych, do której nie ma zastosowania którakolwiek inna podstawa prawna.

Uzasadnione interesy administratora danych / interesy lub prawa podstawowe osoby, której dane dotyczą

Pojęcie „interesu" jest szerszym udziałem, który administrator danych może mieć w przetwarzaniu, lub korzyścią, którą czerpie – lub którą społeczeństwo może czerpać – z przetwarzania. Interes może być bardzo ważny, jasny lub bardziej kontrowersyjny. Sytuacje, o których mowa w art. 7 lit. f), mogą zatem mieć różny zakres – od wykonywania praw podstawowych lub ochrony ważnych interesów osobistych lub społecznych po sytuacje inne, mniej oczywiste, a nawet problematyczne.

Aby można było uznać interes za „uzasadniony" i aby był on istotny na mocy art. 7 lit. f), interes będzie musiał być legalny, tj. zgodny z prawem UE i krajowym. Musi również być wystarczająco jasno sformułowany i szczegółowy, aby umożliwić przeprowadzenie testu równowagi w odniesieniu do interesów i praw podstawowych osoby, której dane dotyczą. Musi także stanowić rzeczywisty i aktualny interes – tj. nie może być oparty na przypuszczeniach.

Jeżeli administrator danych lub osoba trzecia, której dane mają być ujawnione, ma taki uzasadniony interes, niekoniecznie oznacza to, że może powoływać się na art. 7 lit. f) jako podstawę prawną przetwarzania. To, czy można powoływać się na art. 7 lit. f), będzie zależało od wyniku testu równowagi, który zostanie przeprowadzony później. Przetwarzanie musi być również „konieczne dla potrzeb wynikających z uzasadnionych interesów" administratora danych lub – w przypadku ujawniania – osoby trzeciej. Dlatego preferowanym rozwiązaniem zawsze powinny być mniej inwazyjne środki służące temu samemu celowi.

Pojęcie „interesów" osób, których dane dotyczą, jest zdefiniowane jeszcze szerzej, ponieważ nie muszą one być „uzasadnione". Jeżeli administrator danych lub osoba trzecia może realizować jakiekolwiek interesy, pod warunkiem że nie są one nieuzasadnione, to z kolei osoba, której dane dotyczą, ma prawo do tego, żeby uwzględniono wszystkie kategorie jej interesów i porównano je z interesami administratora danych lub osoby trzeciej, o ile interesy tej osoby są istotne w zakresie stosowania dyrektywy.

Stosowanie testu równowagi

Przy interpretacji zakresu stosowania art. 7 lit. f) Grupa Robocza dąży do zrównoważonego podejścia, które zapewnia administratorom danych niezbędną elastyczność w sytuacjach, w których nie ma nadmiernego wpływu na osoby, których dane dotyczą, a jednocześnie zapewnia wystarczającą pewność prawa i daje gwarancje osobom, których dane dotyczą, że ten stwarzający możliwość dowolnej interpretacji przepis nie będzie nieprawidłowo stosowany.

Aby przeprowadzić test równowagi, należy z jednej strony wziąć pod uwagę przede wszystkim charakter i źródło uzasadnionych interesów oraz to, czy przetwarzanie jest konieczne do realizacji tych interesów, a z drugiej strony wpływ na osoby, których dane dotyczą. W tej wstępnej ocenie należy uwzględnić środki, które administrator danych zamierza przyjąć w celu zapewnienia zgodności z dyrektywą, takie jak przejrzystość lub ograniczone gromadzenie danych.

Po przeanalizowaniu i porównaniu obu tych stron można ustalić tymczasową „równowagę": można wyciągnąć wstępny wniosek co do tego, czy uzasadnione interesy administratora danych przeważają nad prawami i interesami osób, których dane dotyczą. Mogą jednak istnieć przypadki, w których wynik testu równowagi jest niejasny i zachodzą wątpliwości, czy uzasadniony interes administratora danych (lub osoby trzeciej) jest nadrzędny i czy podstawą przetwarzania może być art. 7 lit. f).

Z tego powodu ważne jest przeprowadzenie dalszej oceny w ramach testu równowagi. Na tym etapie administrator danych może rozważyć, czy jest w stanie wprowadzić dodatkowe środki, wykraczające poza zapewnienie zgodności z innymi przepisami horyzontalnymi dyrektywy, aby pomóc chronić osoby, których dane dotyczą. Dodatkowe środki mogą obejmować na przykład zapewnienie sprawnego, łatwego w obsłudze i dostępnego mechanizmu, który daje osobom, których dane dotyczą, bezwarunkową możliwość zrezygnowania z przetwarzania.

Kluczowe czynniki, które należy uwzględnić przy stosowaniu testu równowagi

Na podstawie powyższego przydatne czynniki, które należy uwzględnić przy przeprowadzaniu testu równowagi, obejmują:

- <u>charakter i źródło uzasadnionego interesu</u>, w tym:

  - to, czy przetwarzanie danych jest niezbędne do korzystania z prawa podstawowego, lub
  - pod innymi względami leży w interesie publicznym lub jest uznawane w danej społeczności pod względem społecznym, kulturowym lub prawnym/regulacyjnym;

- <u>wpływ na osoby, których dane dotyczą</u>, w tym:

  - charakter danych, na przykład to, czy przetwarzanie obejmuje dane, które mogą być uważane za szczególnie chronione lub które uzyskano z publicznie dostępnych źródeł;
  - sposób, w jaki dane są przetwarzane, w tym, czy dane są podawane do wiadomości publicznej lub w inny sposób udostępniane dużej liczbie osób, lub czy też duże ilości danych osobowych są przetwarzane lub łączone z innymi danymi (np. w przypadku

profilowania, w celach handlowych, w celach egzekwowania prawa lub w innych celach);
- uzasadnione oczekiwania osoby, której dane dotyczą, w szczególności w odniesieniu do wykorzystywania i ujawniania danych w odpowiednim kontekście;
- status administratora danych i osoby, której dane dotyczą, w tym równowaga sił między osobą, której dane dotyczą, a administratorem danych, bądź to, czy osoba, której dane dotyczą, jest dzieckiem lub pod innym względem należy do grupy ludności wymagającej szczególnego traktowania;

- dodatkowe gwarancje mające zapobiegać nadmiernemu wpływowi na osoby, których dane dotyczą, w tym:

  - minimalizacja danych (np. ścisłe ograniczenie gromadzenia danych lub natychmiastowe usunięcie danych po wykorzystaniu);
  - środki techniczne i organizacyjne mające na celu zapewnienie, aby nie można było wykorzystać danych do podejmowania decyzji lub innych działań w stosunku do osób fizycznych („rozdział funkcjonalny”);
  - szerokie wykorzystanie technik anonimizacji, agregacji danych, technologii służących wzmocnieniu ochrony prywatności, uwzględnienia ochrony prywatności już w fazie projektowania, ocen skutków w zakresie ochrony danych i prywatności;
  - większa przejrzystość, ogólne i bezwarunkowe prawo rezygnacji, możliwość przenoszenia danych oraz powiązane środki służące wzmocnieniu pozycji osób, których dane dotyczą.

Rozliczalność, przejrzystość, prawo sprzeciwu oraz dalsze czynniki

Trzy kwestie często odgrywają kluczową rolę w kontekście art. 7 lit. f) w związku z tymi gwarancjami – i ogólną oceną równowagi – i dlatego wymagają szczególnej uwagi:

- istnienie pewnych środków służących zwiększeniu przejrzystości i rozliczalności i ewentualna potrzeba dodatkowych środków w tym zakresie;
- prawo sprzeciwu osoby, której dane dotyczą, wobec przetwarzania oraz, poza sprzeciwem, dostępność mechanizmu rezygnacji bez konieczności uzasadnienia;
- wzmocnienie pozycji osób, których dane dotyczą: możliwość przenoszenia danych oraz dostępność sprawnych mechanizmów umożliwiających osobie, której dane dotyczą, dostęp do jej danych, ich zmienianie, usuwanie, przenoszenie lub dalsze przetwarzanie w inny sposób (lub umożliwiających dalsze przetwarzanie osobom trzecim).

IV. 2. Zalecenia

Obecny tekst art. 7 lit. f) dyrektywy stwarza możliwość dowolnej interpretacji. To elastyczne sformułowanie pozostawia wiele miejsca na interpretację i niekiedy – jak pokazuje doświadczenie – doprowadziło do braku pewności i przewidywalności prawa. Artykuł 7 lit. f), jeżeli jest wykorzystywany w odpowiednim kontekście i przy zastosowaniu odpowiednich kryteriów, określonych w niniejszej opinii, ma jednak istotną rolę do odegrania jako podstawa prawna legalnego przetwarzania danych.

Grupa Robocza popiera zatem obecne podejście przyjęte w art. 6 proponowanego rozporządzenia, w którym równowaga interesów stanowi odrębną podstawę prawną. Dalsze

wytyczne mające na celu zapewnienie odpowiedniego stosowania testu równowagi byłyby jednak przyjęte z zadowoleniem.

Zakres i środki dalszego sprecyzowania

Zasadniczym wymogiem byłoby zachowanie wystarczającej elastyczności tego przepisu oraz dopilnowanie, żeby odzwierciedlał on punkt widzenia zarówno administratora danych, jak i osoby, której dane dotyczą, jak również dynamiczny charakter stosownych kontekstów. Z tego powodu Grupa Robocza jest zdania, że przewidzenie – w tekście proponowanego rozporządzenia lub w aktach delegowanych – szczegółowego i wyczerpującego wykazu sytuacji, w których interes byłby faktycznie zakwalifikowany jako uzasadniony, nie jest wskazane; Grupa Robocza byłaby również przeciwna określeniu przypadków, w których prawo lub interes jednej strony powinny *z zasady* lub *z założenia* być nadrzędne wobec interesu lub prawa drugiej strony jedynie ze względu na charakter takiego interesu lub prawa lub z uwagi na wprowadzenie pewnych środków zabezpieczających, na przykład poddanie danych tylko pseudonimizacji. Stwarzałoby to ryzyko zarówno wprowadzania w błąd przez ten przepis, jak i nadania mu zbyt nakazowego charakteru.

Grupa Robocza nalega na przypisanie *testowi równowagi kluczowej roli* w ocenie na mocy art. 7 lit. f) zamiast formułowania ostatecznych osądów co do istoty różnych praw i interesów. Istnieje potrzeba zachowania elastyczności tego testu, lecz sposób jego przeprowadzania musi stać się skuteczniejszy w praktyce i musi umożliwiać skuteczniejsze przestrzeganie tego przepisu. Powinno to przełożyć się na nałożenie na administratorów danych bardziej rygorystycznego obowiązku *rozliczalności*, w ramach którego administrator danych ponosi odpowiedzialność za *wykazanie*, że interesy i prawa osób, których dane dotyczą, nie mają nadrzędnego charakteru względem jego interesu.

Wytyczne i rozliczalność

Aby osiągnąć ten cel, Grupa Robocza zaleca ujęcie wytycznych w proponowanym rozporządzeniu w następujący sposób.

1) Przydatne byłoby zidentyfikowanie i ujęcie w motywie niepełnego wykazu kluczowych czynników, które należy uwzględnić przy stosowaniu testu równowagi, takich jak: charakter i źródło uzasadnionego interesu, wpływ na osoby, których dane dotyczą, oraz dodatkowe gwarancje, które mogą być zastosowane przez administratora danych w celu uniknięcia nadmiernego wpływu przetwarzania na osoby, których dane dotyczą. Takie gwarancje mogą obejmować m.in.
   - rozdział funkcjonalny danych, właściwe stosowanie technik anonimizacji, szyfrowanie oraz inne środki techniczne i organizacyjne służące ograniczeniu potencjalnego ryzyka dla osób, których dane dotyczą;
   - ale także środki służące zapewnieniu większej przejrzystości i możliwości wyboru osobom, których dane dotyczą, takie jak – w stosownych przypadkach – możliwość bezwarunkowego zrezygnowania z przetwarzania, z której można skorzystać bezpłatnie, łatwo i skutecznie.

2) Grupa Robocza opowiedziałaby się także za zamieszczeniem w proponowanym rozporządzeniu bardziej szczegółowego wyjaśnienia sposobu, w jaki administrator danych mógłby *wykazać*[111] większą rozliczalność.

Zmiana warunków korzystania przez osoby, których dane dotyczą, z prawa sprzeciwu, jak przewidziano w art. 19 proponowanego rozporządzenia, jest już ważnym elementem rozliczalności. Jeżeli osoba, której dane dotyczą, wyraża sprzeciw wobec przetwarzania jej danych na mocy art. 7 lit. f), w ramach proponowanego rozporządzenia to do administratora danych będzie należało wykazanie, że jego interes ma charakter nadrzędny. Grupa Robocza zdecydowanie popiera to odwrócenie ciężaru dowodu, gdyż przyczynia się ono do bardziej rygorystycznego obowiązku rozliczalności.

Jeżeli w konkretnym przypadku administratorowi danych nie uda się wykazać osobie, której dotyczą dane, że jego interes ma charakter nadrzędny, może to również mieć szersze konsekwencje dla całości przetwarzania, nie tylko w odniesieniu do osoby, która wyraziła sprzeciw. W rezultacie administrator danych może zakwestionować przetwarzanie lub podjąć decyzję o jego reorganizacji w stosownych przypadkach – z korzyścią nie tylko dla konkretnej osoby, której dane dotyczą, lecz także dla wszystkich innych osób, których dane dotyczą i które mogą znajdować się w podobnej sytuacji[112].

Wymóg ten jest konieczny, ale nie jest wystarczający. Aby zapewnić ochronę od samego początku i uniknąć obchodzenia przeniesienia ciężaru dowodu[113], ważne jest podjęcie kroków *przed* rozpoczęciem przetwarzania, a nie tylko w trakcie procedury sprzeciwu *ex post*.

Proponuje się zatem, żeby na pierwszym etapie każdego przetwarzania administrator danych musiał podjąć kilka kroków. Pierwsze dwa kroki mogłyby być wymienione w motywie proponowanego rozporządzenia, a trzeci w przepisie szczegółowym:

- należy przeprowadzić ocenę[114], która powinna obejmować różne etapy analizy omówione w niniejszej opinii i podsumowane w załączniku 1. Administrator danych

[111] Takie wykazanie musi pozostawać uzasadnione i być skupione raczej na wyniku, niż na procesie administracyjnym.

[112] Poza odwróceniem ciężaru dowodu Grupa Robocza opowiada się także za tym, żeby proponowane rozporządzenie nie zawierało wymogu, aby sprzeciw był wyrażony z „*ważnych* i uzasadnionych przyczyn dotyczących szczególnej sytuacji" [osoby, której dane dotyczą]. Zgodnie z proponowanym rozporządzeniem wystarczające byłoby raczej odniesienie do wszelkich (niekoniecznie „ważnych") uzasadnionych przyczyn dotyczących szczególnej sytuacji osoby, której dane dotyczą. Kolejną możliwością, która została zaproponowana w sprawozdaniu końcowym komisji LIBE, jest również pozbycie się wymogu, aby sprzeciw musiał odnosić się do szczególnej sytuacji osoby, której dane dotyczą. Grupa Robocza popiera to podejście w tym sensie, że zaleca, aby osoby, których dane dotyczą, były w stanie w stosownych przypadkach korzystać albo z jednej, albo z obu możliwości, tj. albo z możliwości wyrażenia sprzeciwu w oparciu o ich własną szczególną sytuację, albo w bardziej ogólnym zakresie, a w tym ostatnim przypadku bez wymogu podania określonego uzasadnienia. W tym rozumieniu zob. poprawka 114 do art. 19 ust. 1 proponowanego rozporządzenia w sprawozdaniu końcowym komisji LIBE.

[113] Administratorzy danych mogą na przykład mieć pokusę unikania wykazywania w poszczególnych przypadkach, że ich interes jest nadrzędny, używając standardowych form uzasadnienia, lub mogą w inny sposób powodować, że korzystanie z prawa sprzeciwu będzie skomplikowane.

[114] Jak już wspomniano w przypisie 84, oceny tej nie należy mylić z kompleksową oceną skutków w zakresie ochrony danych i prywatności. Obecnie brak jest szczegółowych wytycznych w kwestii ocen wpływu na poziomie europejskim, chociaż w niektórych obszarach, mianowicie w przypadku RFID i inteligentnego pomiaru zużycia energii, podjęto szereg pożytecznych wysiłków na rzecz zdefiniowania metodyki/ram

musiałby wyraźnie określić przedmiotowe nadrzędne interesy oraz wyjaśnić, dlaczego przeważają one nad interesami osób, których dane dotyczą. Taka wstępna ocena nie powinna być zbyt uciążliwa i pozostaje *skalowalna*: może być ograniczona do podstawowych kryteriów, jeżeli wpływ przetwarzania na osoby, których dane dotyczą, jest na pierwszy rzut oka mało znaczący, natomiast z drugiej strony powinna być bardziej dogłębna, jeżeli trudno było osiągnąć równowagę interesów i gdyby równowaga ta wymagała na przykład przyjęcia szeregu dodatkowych gwarancji. W stosownych przypadkach – tj. gdy przetwarzanie stwarza szczególne ryzyko dla praw i wolności osób, których dane dotyczą – należy przeprowadzić bardziej kompleksową ocenę skutków w zakresie ochrony danych i prywatności (na mocy art. 33 proponowanego rozporządzenia), której ważnym elementem mogłaby stać się ocena na mocy art. 7 lit. f).

- należy udokumentować tę ocenę. Podobnie jak *skalowalny* jest poziom szczegółowości oceny, również zakres dokumentacji powinien być skalowalny. Pewna podstawowa dokumentacja powinna jednak być dostępna we wszystkich przypadkach poza tymi najbanalniejszymi, niezależnie od oszacowania wpływu przetwarzania na daną osobę fizyczną. To na podstawie tej dokumentacji możliwe jest dalsze przeanalizowanie oceny dokonanej przez administratora danych i ewentualnie jej zakwestionowanie;

- należy zapewnić przejrzystość i widoczność tych informacji w odniesieniu do osób, których dane dotyczą, i innych zainteresowanych stron. Należy zapewnić przejrzystość zarówno wobec osób, których dane dotyczą, jak i organów ochrony danych, oraz w stosownych przypadkach ogółu społeczeństwa. Jeżeli chodzi o osoby, których dane dotyczą, Grupa Robocza przywołuje projekt sprawozdania komisji LIBE[115], w którym stwierdzono, że administrator danych powinien poinformować osobę, której dane dotyczą, o powodach uznania, że interes administratora danych nie ma charakteru podrzędnego względem interesów lub podstawowych praw i wolności osoby, której dane dotyczą. Zdaniem Grupy Roboczej takie informacje powinny być udzielane osobom, których dane dotyczą, wraz z informacjami, które administrator danych musi przekazać na mocy z art. 10 i 11 obecnej dyrektywy (art. 11 proponowanego rozporządzenia). Pozwoli to na ewentualne wyrażenie sprzeciwu przez osobę, której dane dotyczą, w ramach drugiego kroku oraz przedstawienie w

---

sektorowych (lub szablonu), które mogłyby być stosowane w całej Unii Europejskiej. Zob. „Propozycja sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID" oraz „Szablon oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych", opracowane przez grupę ekspertów nr 2 w ramach grupy zadaniowej ds. inteligentnych sieci Komisji. Grupa Robocza wydała kolejne opinie dotyczące obu tych metodyk.
Ponadto podjęto inicjatywy na rzecz określenia ogólnej metodyki oceny skutków w zakresie ochrony danych, które to działania mogą pomóc w wysiłkach typowych dla tego obszaru. Zob. np. Projekt PIAF (Ramy oceny skutków w zakresie prywatności w odniesieniu do praw do ochrony danych i do prywatności): http://www.piafproject.eu/
W kwestii wytycznych na poziomie krajowym zob. np. metodyka CNIL:
http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
oraz podręcznik ICO dotyczący oceny skutków w zakresie prywatności:
http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf

[115] Projekt sprawozdania odnoszącego się do 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)).

poszczególnych przypadkach przez administratora danych dodatkowego uzasadnienia dotyczącego przeważających interesów. Ponadto dokumentacja, na której administrator danych oparł swoją ocenę, powinna być na żądanie udostępniana organom ochrony danych w celu umożliwienia ewentualnej weryfikacji i egzekwowania w stosownych przypadkach.

Grupa Robocza opowiedziałaby się także za wyraźnym uwzględnieniem tych trzech kroków w proponowanym rozporządzeniu w sposób określony powyżej. Byłoby to uznaniem szczególnej roli podstaw prawnych w ocenie legalności i sprecyzowałoby znaczenie testu równowagi w szerszym kontekście środków rozliczalności i ocen skutków w proponowanych nowych ramach prawnych.

Grupa Robocza uważa, że wskazane jest również powierzenie Europejskiej Radzie Ochrony Danych zadania polegającego na zapewnieniu dalszych wytycznych w razie potrzeby na podstawie tych ram. Takie podejście pozwoliłoby zarówno na dostateczną jasność tekstu tych ram, jak i na wystarczającą elastyczność pod względem ich wdrożenia.

Załącznik 1. Krótki poradnik na temat sposobu przeprowadzania testu równowagi na mocy art. 7 lit. f)

Krok 1: Ocena, która podstawa prawna może potencjalnie mieć zastosowanie na mocy art. 7 lit. a)–f)

Przetwarzanie danych może być realizowane tylko wtedy, gdy ma zastosowanie co najmniej jedna z sześciu podstaw określonych w art. 7 lit. a)–f) (na różnych etapach tego samego przetwarzania można przywoływać różne podstawy). Jeśli na pierwszy rzut oka wydaje się, że art. 7 lit. f) mógłby stanowić odpowiednią podstawę prawną, należy przejść do kroku 2.

Krótkie wskazówki:

- art. 7 lit. a) ma zastosowanie tylko wtedy, gdy wyrażono dobrowolną, świadomą, konkretną i jednoznaczną zgodę; tego, że dana osoba fizyczna nie zgłosiła sprzeciwu wobec przetwarzania na mocy art. 14, nie należy mylić ze zgodą, o której mowa w art. 7 lit. a) – jednak prosty mechanizm wyrażenia sprzeciwu wobec przetwarzania może być uznany za istotną gwarancję na mocy art. 7 lit. f);
- art. 7 lit. b) obejmuje przetwarzanie, które jest konieczne dla realizacji umowy; samo to, że przetwarzanie danych jest związane z umową lub przewidziane w warunkach umowy, niekoniecznie oznacza, że podstawa ta ma zastosowanie; w stosownych przypadkach należy rozważyć art. 7 lit. f) jako alternatywę;
- art. 7 lit. c) dotyczy tylko wyraźnych i konkretnych zobowiązań prawnych wynikających z prawa UE lub państwa członkowskiego; w przypadku niewiążących wytycznych (na przykład wydanych przez agencje regulacyjne) lub zagranicznego zobowiązania prawnego należy rozważyć art. 7 lit. f) jako alternatywę.

Krok 2: Kwalifikacja interesu jako „uzasadnionego" lub „nieuzasadnionego"

Aby można było uznać interes za uzasadniony, musi on łącznie spełniać następujące warunki:

- być legalny (tj. zgodny z prawem UE i krajowym);
- być wystarczająco jasno sformułowany, aby umożliwić przeprowadzenie testu równowagi w odniesieniu do interesów i praw podstawowych osoby, której dane dotyczą (tj. wystarczająco konkretny);
- stanowić rzeczywisty i aktualny interes (tj. nie może być oparty na przypuszczeniach).

Krok 3: Ustalenie, czy przetwarzanie jest konieczne dla realizacji zamierzonego interesu

Aby spełnić ten wymóg, należy rozważyć, czy istnieją inne, mniej inwazyjne środki służące osiągnięciu określonego celu przetwarzania i realizacji uzasadnionego interesu administratora danych.

Krok 4: Ustalenie tymczasowej równowagi poprzez ocenienie, czy podstawowe prawa i interesy osób, których dane dotyczą, przeważają nad interesem administratora danych

- rozważyć charakter interesów administratora danych (prawo podstawowe, inny rodzaj interesu, interes publiczny);
- ocenić ewentualne szkody poniesione przez administratora danych, osoby trzecie lub szerszą społeczność, jeżeli przetwarzanie danych nie ma miejsca;

- uwzględnić charakter danych (dane szczególnie chronione w sensie ścisłym czy szerszym?);
- rozważyć status osoby, której dane dotyczą (nieletni, pracownik itp.), i administratora danych (np. czy organizacja przedsiębiorstw ma dominującą pozycję na rynku);
- uwzględnić sposób przetwarzania danych (na dużą skalę, eksploracja danych, profilowanie, ujawnianie wielu osobom lub publikacja);
- określić podstawowe prawa lub interesy osoby, której dane dotyczą, na które przetwarzanie może mieć wpływ;
- rozważyć uzasadnione oczekiwania osób, których dane dotyczą;
- ocenić wpływ na osobę, której dane dotyczą, i porównać go z korzyściami z przetwarzania oczekiwanymi przez administratora danych.

Krótka wskazówka: należy rozważyć skutki faktycznego przetwarzania dla poszczególnych osób fizycznych – nie traktować tego jako zadania abstrakcyjnego lub hipotetycznego.

Krok 5: Ustalenie ostatecznej równowagi poprzez uwzględnienie dodatkowych gwarancji

Należy określić i wdrożyć odpowiednie dodatkowe gwarancje wynikające z obowiązku dochowania należytej staranności, takie jak:
- minimalizacja danych (np. ścisłe ograniczenie gromadzenia danych lub natychmiastowe usunięcie danych po wykorzystaniu);
- środki techniczne i organizacyjne mające na celu zapewnienie, aby nie można było wykorzystać danych do podejmowania decyzji lub innych działań w stosunku do osób fizycznych („rozdział funkcjonalny”);
- szerokie wykorzystanie technik anonimizacji, agregacji danych, technologii służących wzmocnieniu ochrony prywatności, uwzględnienia ochrony prywatności już w fazie projektowania, ocen skutków w zakresie ochrony danych i prywatności;
- większa przejrzystość, ogólne i bezwarunkowe prawo sprzeciwu (rezygnacji), możliwość przenoszenia danych oraz powiązane środki służące wzmocnieniu pozycji osób, których dane dotyczą.

Krótka wskazówka: stosowanie rodzajów podejścia i technologii służących wzmocnieniu ochrony prywatności może przechylić szalę na korzyść administratora danych, a także chronić osoby fizyczne.

Krok 6: Wykazanie zgodności i zapewnienie przejrzystości

- sporządzić plan kroków 1–5 w celu uzasadnienia przetwarzania przed jego rozpoczęciem;
- poinformować osoby, których dane dotyczą, o powodach uznania, że szala przechyla się na stronę administratora danych;
- zachować dokumentację do dyspozycji organów ochrony danych.

Krótka wskazówka: Ten krok jest *skalowalny* – szczegóły oceny i dokumentacji należy dostosować do charakteru i kontekstu przetwarzania. Środki te będą szerzej zakrojone w przypadku przetwarzania dużej ilości informacji na temat wielu osób w sposób sprawiający, że przetwarzanie to może mieć na nie znaczny wpływ. Kompleksowa ocena skutków w zakresie ochrony danych i prywatności (na mocy art. 33 proponowanego rozporządzenia) będzie konieczna tylko wtedy, gdy czynność przetwarzania stwarza konkretne ryzyko dla praw i wolności osób, których dane dotyczą. W takich przypadkach ocena na mocy 7 lit. f) może stać się kluczowym elementem tej szerszej oceny skutków.

Krok 7: Co się dzieje, jeżeli osoba, której dane dotyczą, korzysta z prawa sprzeciwu?

- jeżeli jako gwarancja dostępne jest tylko kwalifikowane prawo do rezygnacji (jest to wyraźnie wymagane na mocy art. 14 lit. a) jako minimalna gwarancja): w przypadku gdy osoba, której dane dotyczą, wyraża sprzeciw wobec przetwarzania, należy zapewnić, aby istniał odpowiedni i łatwy w obsłudze mechanizm umożliwiający ponowne ocenienie równowagi w odniesieniu do danej osoby fizycznej i zaprzestanie przetwarzania jej danych, jeżeli ponowna ocena pokazuje, że interesy tej osoby przeważają;
- jeżeli bezwarunkowe prawo do rezygnacji jest gwarancją dodatkową (ponieważ jest to albo wyraźnie wymagane na mocy art. 14 lit. b), albo ponieważ z innych względów uznano to za konieczną lub pomocną gwarancję dodatkową): w przypadku gdy osoba, której dane dotyczą, wyraża sprzeciw wobec przetwarzania, należy zapewnić poszanowanie tej decyzji bez potrzeby podejmowania dalszych kroków lub przeprowadzania dalszych ocen.

Załącznik 2. Praktyczne przykłady ilustrujące stosowanie testu równowagi na mocy art. 7 lit. f)

Niniejszy załącznik zawiera przykłady pewnych najczęstszych sytuacji, w których może pojawić się kwestia uzasadnionego interesu w rozumieniu art. 7 lit. f). W większości przypadków pogrupowano po co najmniej dwa podobne przykłady, które warto porównać w tym samym punkcie. Wiele przykładów opiera się na rzeczywistych przypadkach lub elementach rzeczywistych przypadków rozpatrywanych przez organy ochrony danych w różnych państwach członkowskich. Niekiedy jednak w pewnym stopniu zmieniono fakty, aby lepiej zilustrować sposób przeprowadzania testu równowagi.

Przykłady przedstawiono w celu zilustrowania *procesu myślenia* – metody, którą należy zastosować w celu przeprowadzenia testu równowagi w oparciu o wiele czynników. Innymi słowy, przykłady te *nie* mają na celu zapewnienia *jednoznacznej* oceny opisanych przypadków. Co więcej, w wielu przypadkach pewna zmiana okoliczności (na przykład gdyby administrator danych miał przyjąć dodatkowe gwarancje, takie jak pełniejsza anonimizacja, lepsze środki bezpieczeństwa oraz większa przejrzystość i bardziej rzeczywisty wybór dla osób, których dane dotyczą) mogłaby spowodować zmianę wyniku testu równowagi[116].

Powinno to zachęcić administratorów danych do lepszego przestrzegania wszystkich przepisów horyzontalnych dyrektywy i oferowania dodatkowej ochrony w razie potrzeby w oparciu o prywatność i uwzględnienie ochrony danych już w fazie projektowania. Im bardziej administratorzy danych zadbają o ogólną ochronę danych osobowych, tym bardziej prawdopodobne jest, że pozytywnie przejdą test równowagi.

Korzystanie z prawa do wolności wypowiedzi i informacji[117], w tym w mediach i sztuce

Przykład 1: Organizacja pozarządowa ponownie publikuje informacje na temat wydatków parlamentarzystów

Organ publiczny publikuje – na mocy zobowiązania prawnego (art. 7 lit. c)) – wydatki parlamentarzystów; organizacja pozarządowa działająca na rzecz przejrzystości z kolei analizuje i ponownie publikuje te dane w wersji dokładnej i proporcjonalnej, ale bardziej informacyjnej, gdyż opatrzonej adnotacjami, co przyczynia się do większej przejrzystości i rozliczalności.

Zakładając, że organizacja pozarządowa ponownie publikuje informacje i opatruje je adnotacjami w sposób dokładny i proporcjonalny, przyjmuje odpowiednie gwarancje oraz – w szerszym ujęciu – nie narusza praw osób, których dane dotyczą, powinna być w stanie powołać się na art. 7 lit. f) jako podstawę prawną przetwarzania. Takie czynniki, jak:

[116] Prawidłowe stosowanie art. 7 lit. f) może wiązać się ze skomplikowanymi kwestiami oceny. Ważną rolę mogą odgrywać szczegółowe przepisy, orzecznictwo, praktyka sądowa, wytyczne oraz kodeksy postępowania i inne formalne lub mniej formalne standardy, które mogą być pomocne w przeprowadzeniu tej oceny.

[117] Wolność wypowiedzi i informacji – zob. s. 38 niniejszej opinii. Przy analizowaniu tych przykładów trzeba również wziąć pod uwagę wszelkie istotne odstępstwa na mocy prawa krajowego dotyczące przetwarzania w celach dziennikarskich na mocy art. 9 dyrektywy.

charakter uzasadnionego interesu (podstawowe prawo do wolności wypowiedzi i informacji), interes publiczny leżący w przejrzystości i rozliczalności oraz fakt, że dane zostały już opublikowane i odnoszą się do (stosunkowo mniej chronionych) danych osobowych związanych z działalnością osób istotną dla wykonywania ich funkcji publicznych[118], przemawiają za legalnością przetwarzania. Fakt, że pierwsza publikacja danych była wymagana przez prawo oraz że zainteresowane osoby powinny więc spodziewać się, że ich dane zostaną opublikowane, także przyczynia się do pozytywnej oceny. Po drugiej stronie tej równowagi istnieją skutki dla osób zainteresowanych, które mogą być znaczne, na przykład ze względu na kontrolę publiczną integralność osobista niektórych osób może być kwestionowana, co może prowadzić przykładowo do przegranej w wyborach lub w niektórych przypadkach do dochodzeń w sprawie oszustw. Powyższe czynniki razem wzięte pokazują jednak, że w równowadze tej interesy administratora danych (i interesy społeczeństwa, któremu dane są ujawniane) są ważniejsze niż interesy osób, których dane dotyczą.

Przykład 2: Lokalny radny mianuje swoją córkę na stanowisko specjalnego asystenta

Dziennikarz publikuje w lokalnej gazecie internetowej zgodny z faktami, rzetelny artykuł o lokalnym radnym, ujawniając, że wziął on udział tylko w jednym z ostatnich jedenastu posiedzeń rady oraz prawdopodobnie nie zostanie ponownie wybrany na radnego z powodu niedawnego skandalu związanego z mianowaniem jego siedemnastoletniej córki na stanowisko specjalnego asystenta.

W tym przypadku ma zastosowanie analiza podobna do tej z *przykładu 1*. Jeżeli chodzi o fakty, to publikowanie tych informacji leży w uzasadnionych interesach danej gazety. Mimo że ujawniono dane osobowe radnego, jego prawo do prywatności nie przeważa nad podstawowym prawem do wolności wypowiedzi i do opublikowania przedmiotowego artykułu w gazecie. Wynika to z tego, że prawo do prywatności osób publicznych jest stosunkowo ograniczone pod względem ich działalności publicznej, oraz ze szczególnego znaczenia wolności wypowiedzi – zwłaszcza w przypadku gdy publikacja artykułu leży w interesie publicznym.

Przykład 3: W pierwszych wynikach wyszukiwania ciągle figuruje drobne przestępstwo

Internetowe archiwum gazety zawiera stary artykuł dotyczący pewnej osoby, kiedyś lokalnej znakomitości, kapitana amatorskiej drużyny piłkarskiej z małego miasta. W artykule podano pełne imię i nazwisko tej osoby, a dotyczy on jej udziału w stosunkowo mało istotnym postępowaniu karnym (w sprawie naruszenia porządku publicznego w stanie nietrzeźwym). Kartoteka kryminalna tej osoby jest obecnie czysta i nie figuruje już w niej dawne przestępstwo, za które osoba ta odbyła karę kilka lat temu. Osobę tę najbardziej niepokoi fakt, że przy wyszukiwaniu jego imienia i nazwiska za pomocą popularnych wyszukiwarek internetowych jednym z pierwszych wyników jest link do tego starego artykułu. Pomimo prośby gazeta odmawia przyjęcia środków technicznych, które ograniczyłyby szerszą

[118] Nie można wykluczyć, że niektóre wydatki mogą ujawniać dane szczególnie chronione, takie jak dane dotyczące zdrowia. W takim przypadku wydatki te powinny być usunięte ze zbioru danych, zanim zostanie on opublikowany po raz pierwszy. Dobrą praktyką jest przyjęcie „aktywnego podejścia" i zapewnienie osobom fizycznym możliwość wglądu w swoje dane przed ich publikacją oraz wyraźne poinformowanie ich o możliwościach i sposobach publikacji.

dostępność przedmiotowego artykułu na temat osoby, której dane dotyczą. Gazeta odmawia na przykład przyjęcia środków technicznych i organizacyjnych, które służyłyby – w zakresie, w jakim pozwala na to technologia – ograniczeniu dostępu do tych informacji podczas używania w zewnętrznej wyszukiwarce imienia i nazwiska danej osoby jako kategorii wyszukiwania.

Jest to kolejny przypadek ilustrujący możliwy konflikt między wolnością wypowiedzi a prywatnością. Pokazuje również, że w niektórych sytuacjach dodatkowe gwarancje – takie jak zapewnienie, aby, przynajmniej w przypadku uzasadnionego sprzeciwu na mocy art. 14 lit. a) dyrektywy, odpowiednia część archiwów prasowych nie była już dostępna za pośrednictwem zewnętrznych wyszukiwarek lub aby format używany do wyświetlania informacji nie pozwalał na wyszukiwanie według imienia i nazwiska – mogą odgrywać kluczową rolę w osiągnięciu właściwej równowagi pomiędzy tymi dwoma prawami podstawowymi. Pozostaje to bez uszczerbku dla wszelkich innych środków, które mogą podjąć wyszukiwarki lub inne osoby trzecie[119].

Konwencjonalny marketing bezpośredni i inne formy marketingu lub reklamy

Przykład 4: Sklep komputerowy reklamuje wśród klientów podobne produkty

Sklep komputerowy pozyskuje od swoich klientów dane kontaktowe w kontekście sprzedaży produktu i wykorzystuje te dane na potrzeby marketingu własnych podobnych produktów za pośrednictwem poczty konwencjonalnej. Sklep sprzedaje również produkty w Internecie i rozsyła promocyjne wiadomości e-mail, gdy nowa linia produktów wchodzi do sprzedaży. Klienci są wyraźnie informowani o możliwości wyrażenia sprzeciwu bezpłatnie i w łatwy sposób, kiedy ich dane kontaktowe są gromadzone, oraz przy okazji każdej wysłanej wiadomości, jeżeli klient początkowo nie wyraził sprzeciwu.

Przejrzystość przetwarzania, fakt, że klient może w normalnych okolicznościach spodziewać się otrzymywania ofert dotyczących podobnych produktów jako klient danego sklepu, oraz fakt, że klient ma prawo sprzeciwu, przyczynia się do legalności przetwarzania i ochrony praw osób fizycznych. Jeżeli chodzi o drugą stronę równowagi, wydaje się, że nie ma nieproporcjonalnego wpływu na prawo do prywatności (w tym przykładzie założono, że sklep komputerowy nie tworzy żadnych skomplikowanych profili swoich klientów, na przykład przy użyciu szczegółowej analizy danych dotyczących kliknięć).

Przykład 5: Internetowa apteka przeprowadza rozległe profilowanie

Marketing internetowej apteki prowadzony jest na podstawie zakupionych przez klientów leków i innych produktów, w tym produktów na receptę. Informacje te są analizowane – w połączeniu z informacjami demograficznymi na temat klientów, na przykład ich wieku i płci – w celu tworzenia profilu „zdrowia i dobrego samopoczucia" poszczególnych klientów. Wykorzystywane są również dane dotyczące kliknięć. Dane te są gromadzone nie tylko w odniesieniu do produktów zakupionych przez klientów, ale także na temat innych produktów i informacji, które przeglądali na stronie internetowej. Profile klientów zawierają informacje lub prognozy sugerujące, że dany klient jest w ciąży, cierpi na określoną chorobę przewlekłą lub byłby zainteresowany zakupem suplementów diety, kremu do opalania lub innych

[119] Zob. także sprawa C-131/12 Google Spain przeciwko Agencia Española de Proteccion de Datos, obecnie tocząca się przed Trybunałem Sprawiedliwości Unii Europejskiej.

produktów do pielęgnacji skóry w określonych porach roku. Analitycy apteki internetowej wykorzystują te informacje w celu oferowania poszczególnym osobom leków bez recepty, suplementów zdrowotnych i innych produktów za pośrednictwem poczty elektronicznej. W tym przypadku apteka nie może powoływać się na swoje uzasadnione interesy, kiedy tworzy profile swoich klientów i korzystania z nich na potrzeby marketingu. Z opisanym profilowaniem wiąże się kilka problemów. Przedmiotowe informacje stanowią dane szczególnie chronione i mogą ujawniać bardzo dużo o sprawach, co do których wiele osób oczekiwałoby, że pozostaną prywatne[120]. Zakres i sposób profilowania (wykorzystywanie danych dotyczących kliknięć, algorytmy predykcyjne) również wskazują na wysoki stopień ingerencji. W stosownych przypadkach za alternatywne rozwiązanie można byłoby jednak uznać zgodę na podstawie art. 7 lit. a) i art. 8 ust. 2 lit. a) (jeżeli przetwarzane są dane szczególnie chronione).

Niezamówione wiadomości niehandlowe, w tym na potrzeby kampanii politycznych lub zbierania środków na cele charytatywne

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

Kandydatka w wyborach lokalnych wykorzystuje spis wyborców[121], aby przesłać każdemu potencjalnemu wyborcy w swoim okręgu wyborczym list wprowadzający promujący jej kampanię w nadchodzących wyborach. Kandydatka wykorzystuje dane uzyskane ze spisu wyborców tylko do wysłania tego listu i nie zatrzymuje danych po zakończeniu kampanii.

Takie wykorzystanie lokalnego spisu mieści się w uzasadnionych oczekiwaniach osób, kiedy odbywa się w okresie przedwyborczym – interes administratora danych jest jasny i uzasadniony. Ograniczone i ukierunkowane wykorzystanie informacji przyczynia się także do przechylenia szali na korzyść uzasadnionego interesu administratora danych. Takie wykorzystanie spisów wyborców może być również regulowane przez prawo na poziomie krajowym, z punktu widzenia interesu publicznego, poprzez szczegółowe przepisy, ograniczenia i gwarancje w odniesieniu do korzystania ze spisu wyborców. Jeżeli w tym przypadku ma to miejsce, do zapewnienia legalności przetwarzania wymagana jest również zgodność z tymi szczegółowymi przepisami.

Przykład 7: Organizacja nienastawiona na zysk gromadzi informacje na potrzeby kierowania treści do określonego odbiorcy

Organizacja filozoficzna oddana rozwojowi społecznemu postanawia organizować działania w zakresie pozyskiwania środków w oparciu o profil swoich członków. W tym celu gromadzi dane na portalach społecznościowych za pomocą oprogramowania ad hoc ukierunkowanego na osoby, które „polubiły" stronę organizacji, „polubiły" lub „udostępniły" wiadomość zamieszczoną przez organizację na jej stronie, regularnie przeglądały niektóre pozycje lub zamieściły na Twitterze wiadomości organizacji. Następnie rozsyła wiadomości i biuletyny

[120] Poza ograniczeniami przewidzianymi w przepisach o ochronie danych reklamowanie produktów wydawanych na receptę również jest ściśle regulowane w UE, a istnieją także pewne ograniczenia dotyczące reklamowania leków dostępnych bez recepty. Ponadto trzeba również uwzględnić wymogi określone w art. 8 w odniesieniu do szczególnych kategorii danych (takich jak dane dotyczące zdrowia).

[121] Zakłada się, że w państwie członkowskim, którego dotyczy przykład, spis wyborców jest ustanowiony na podstawie prawa.

wśród swoich członków zgodnie z ich profilami. Na przykład starsi właściciele psów, którzy „polubili" artykuły na temat schronisk dla zwierząt, otrzymują różne prośby o pomoc pieniężną na rzecz rodzin z małymi dziećmi; osoby z różnych grup etnicznych także otrzymują różne wiadomości.

Fakt, że przetwarzane są szczególne kategorie danych (przekonania filozoficzne), wymaga zgodności z art. 8, który to warunek wydaje się spełniony, gdyż przetwarzanie odbywa się w ramach legalnej działalności organizacji. W tym przypadku nie jest to jednak warunek wystarczający: sposób wykorzystywania danych przekracza uzasadnione oczekiwania osób fizycznych. Ilość gromadzonych danych, brak przejrzystości w zakresie gromadzenia oraz ponowne wykorzystywanie w innym celu danych pierwotnie opublikowanych w jednym celu przyczyniają się do wniosku, że w tym przypadku nie można powoływać się na art. 7 lit. f). Przetwarzanie nie powinno zatem być dozwolone, chyba że można oprzeć się na innej podstawie, na przykład zgodzie na mocy art. 7 lit. a).

Egzekwowanie roszczeń prawnych, w tym windykacja należności poprzez postępowanie pozasądowe

Przykład 8: Spór o jakość prac remontowych

Klient kwestionuje jakość prac remontowych przeprowadzonych w kuchni i nie chce zapłacić pełnej należności. Przedsiębiorstwo budowlane przekazuje odpowiednie i proporcjonalne dane swojemu prawnikowi, aby mógł przypomnieć klientowi o płatności i wynegocjować z nim ugodę, jeśli klient nadal będzie odmawiał zapłaty.

W tym przypadku wstępne działania podjęte przez przedsiębiorstwo budowlane w oparciu o podstawowe informacje na temat osoby, której dane dotyczą (np. imię i nazwisko, adres, numer umowy), w celu przesłania tej osobie upomnienia (bezpośrednio lub za pośrednictwem swojego adwokata, jak w tej sytuacji) nadal mogą wchodzić w zakres przetwarzania koniecznego dla realizacji umowy (art. 7 lit. b)). Podjęte dalsze kroki[122], łącznie z zaangażowaniem firmy windykacyjnej, należy jednak ocenić na mocy art. 7 lit. f), biorąc pod uwagę między innymi ich stopień ingerencji i wpływ na osobę, której dane dotyczą. Zostanie to pokazane w poniższym przykładzie.

Przykład 9: Klient znika z samochodem zakupionym na kredyt

Klient nie płaci należnych rat za drogi sportowy samochód zakupiony na kredyt, a następnie „znika". Dealer samochodowy zawiera umowę z windykatorem będącym osobą trzecią. Windykator ten przeprowadza inwazyjne dochodzenie w stylu organów ścigania, wykorzystując między innymi takie praktyki, jak niejawny nadzór wideo i podsłuch telefoniczny.

Chociaż interesy dealera samochodowego i windykatora są uzasadnione, szala nie przechyla się na jego stronę ze względu na inwazyjne metody – z których część jest wyraźnie zabroniona przez prawo (podsłuch telefoniczny) – stosowane w celu gromadzenia informacji.

[122] Obecnie w państwach członkowskich istnieją pewne różnice co do tego, które środki mogą być uważane za konieczne dla realizacji umowy.

Wniosek byłby inny, gdyby na przykład dealer samochodowy lub windykator przeprowadzili tylko ograniczone kontrole, aby potwierdzić dane kontaktowe osoby, której dane dotyczą, w celu wszczęcia postępowania przed sądem.

Zapobieganie oszustwom, niewłaściwemu wykorzystywaniu usług lub praniu pieniędzy

Przykład 10: Weryfikacja danych klienta przed otwarciem rachunku bankowego

Instytucja finansowa stosuje uzasadnione i proporcjonalne procedury – zgodne z niewiążącymi wytycznymi właściwego publicznego organu nadzoru finansowego – w celu zweryfikowania tożsamości każdej osoby ubiegającej się o otwarcie rachunku. Prowadzi rejestr informacji wykorzystanych do zweryfikowania tożsamości.

Interes administratora danych jest uzasadniony, a przetwarzanie danych obejmuje tylko ograniczone i niezbędne informacje (co jest standardową praktyką w tym sektorze, zasadnie oczekiwaną przez osoby, których dane dotyczą, i zalecaną przez właściwe organy). Istnieją odpowiednie granice służące ograniczeniu nieproporcjonalnego i nadmiernego wpływu na osoby, których dane dotyczą. Administrator danych może zatem powoływać się na art. 7 lit. f). Ewentualnie mógłby stosować się art. 7 lit. c) – o ile podjęte działania są wyraźnie wymagane w prawie właściwym.

Przykład 11: Wymiana informacji w celu zwalczania prania pieniędzy

Instytucja finansowa – po uzyskaniu porady właściwego organu ochrony danych – wdraża procedury oparte na konkretnych, ograniczonych kryteriach na potrzeby wymiany danych dotyczących podejrzewanego nadużywania przepisów dotyczących przeciwdziałania praniu pieniędzy. Wymiana ta odbywa się z innymi przedsiębiorstwami w ramach tej samej grupy. Obowiązuje ścisłe ograniczenie dostępu, środki bezpieczeństwa i zakaz dalszego wykorzystywania danych w innych celach.

Z powodów podobnych do tych wyjaśnionych powyżej oraz w zależności od okoliczności danego przypadku podstawą przetwarzania danych mógłby być art. 7 lit. f). Ewentualnie mógłby stosować się art. 7 lit. c) – o ile podjęte działania są wyraźnie wymagane w prawie właściwym.

Przykład 12: Czarna lista agresywnych narkomanów

Grupa szpitali tworzy wspólną czarną listę „agresywnych" osób poszukujących narkotyków, aby zakazać tym osobom dostępu do wszystkich pomieszczeń medycznych w tych szpitalach.

Nawet jeśli interes administratorów danych leżący w utrzymywaniu bezpiecznych lokali jest uzasadniony, trzeba go rozważyć w kontekście podstawowego prawa do prywatności i innych istotnych kwestii, takich jak potrzeba niewykluczania zainteresowanych osób z dostępu do opieki zdrowotnej. Fakt przetwarzania danych szczególnie chronionych (np. danych dotyczących zdrowia związanych z narkomanią) również potwierdza wniosek, że w tym

przypadku jest mało prawdopodobne, aby przetwarzanie było dopuszczalne na mocy art. 7 lit. f)[123]. Przetwarzanie mogłoby być dopuszczalne, gdyby było na przykład uregulowane przepisami przewidującymi konkretne gwarancje (kontrole, przejrzystość, zapobieganie zautomatyzowanym decyzjom), które zapewniałyby, aby przetwarzanie nie prowadziło do dyskryminacji osób fizycznych lub naruszenia ich praw podstawowych[124]. W tym ostatnim przypadku, w zależności od tego, czy w tych szczególnych przepisach przetwarzanie byłoby wymagane, czy tylko dozwolone, podstawę prawną może stanowić art. 7 lit. c) lub f).

Monitorowanie pracowników dla celów bezpieczeństwa lub zarządzania

Przykład 13: Godziny pracy prawników wykorzystywane zarówno do celów fakturowania, jak i premii

Liczba fakturowanych godzin przepracowanych przez prawników w kancelarii jest przetwarzana zarówno dla celów fakturowania, jak i na potrzeby ustalenia wysokości premii rocznych. System jest w przejrzysty sposób wyjaśniony pracownikom, którzy mają jednoznaczne prawo do wyrażenia sprzeciwu wobec wniosków wyciągniętych zarówno w zakresie fakturowania, jak i premii, a następnie omówienia tych kwestii z kierownictwem.

Przetwarzanie wygląda na konieczne dla uzasadnionych interesów administratora danych i wydaje się, że nie istnieje mniej inwazyjny sposób osiągnięcia założonego celu. Wpływ na pracowników jest również ograniczony dzięki wprowadzonym gwarancjom i procesom. Artykuł 7 lit. f) mógłby być zatem odpowiednią podstawą prawną w tym przypadku. Można również wysunąć argument uzasadniający to przetwarzanie w jednym celu lub w obu celach jako konieczne dla realizacji umowy.

Przykład 14: Elektroniczne monitorowanie korzystania z Internetu[125]

Pracodawca monitoruje korzystanie przez pracowników z Internetu w czasie pracy, aby sprawdzić, czy nie korzystają nadmiernie z Internetu w celach osobistych. Gromadzone dane obejmują pliki tymczasowe i pliki cookie generowane na komputerach pracowników, które pokazują odwiedzone strony internetowe i treści pobrane w godzinach pracy. Dane te są przetwarzane bez wcześniejszej konsultacji z osobami, których dane dotyczą, oraz z przedstawicielami związków zawodowych/rady zakładowej w danym przedsiębiorstwie. Zainteresowanym osobom nie udziela się również wystarczających informacji o tych praktykach.

Ilość i charakter gromadzonych danych wskazują na istotną ingerencję w życie prywatne pracowników. Ważnym czynnikiem, który należy uwzględnić, jest oprócz kwestii proporcjonalności także przejrzystość tych praktyk, która jest ściśle związana z uzasadnionymi oczekiwaniami osób, których dane dotyczą. Nawet jeżeli pracodawca ma

[123] Trzeba również uwzględnić wymogi określone w art. 8 w odniesieniu do szczególnych kategorii danych (takich jak dane dotyczące zdrowia).

[124] Zob. dokument roboczy w sprawie czarnych list (WP 65), przyjęty w dniu 3 października 2002 r.

[125] Kilka państw członkowskich uważa, że pewne ograniczone monitorowanie elektroniczne może być „konieczne dla realizacji umowy", a zatem jego podstawą prawną może być raczej art. 7 lit. b) niż art. 7 lit. f).

uzasadniony interes leżący w ograniczeniu ilości czasu przeznaczanego przez pracowników na odwiedzanie stron internetowych, które nie mają bezpośredniego znaczenia dla ich pracy, stosowane metody nie spełniają testu równowagi na mocy art. 7 lit. f). Pracodawca powinien stosować metody mniej inwazyjne (np. ograniczenie dostępu do określonych stron), które są jako najlepsze praktyki omówione i uzgodnione z przedstawicielami pracowników i o których pracownicy są w przejrzysty sposób poinformowani.

Systemy informowania o nieprawidłowościach

Przykład 15: System informowania o nieprawidłowościach na potrzeby spełniania zagranicznych zobowiązań prawnych

Unijny oddział amerykańskiej grupy tworzy ograniczony system informowania o nieprawidłowościach na potrzeby zgłaszania poważnych naruszeń w zakresie księgowości i finansów. Podmioty grupy podlegają kodeksowi dobrego zarządzania, w którym wymaga się wzmocnienia procedur kontroli wewnętrznej i zarządzania ryzykiem. Ze względu na swoją działalność międzynarodową oddział unijny ma obowiązek dostarczać wiarygodne dane finansowe innym członkom grupy w Stanach Zjednoczonych. Wspomniany system ma być zgodny zarówno z prawem Stanów Zjednoczonych, jak i z wytycznymi krajowych organów ochrony danych w UE.

W ramach gwarancji pracownicy otrzymują – poprzez szkolenia i inne metody – jasne wytyczne co do okoliczności, w których należy korzystać z tego systemu. Pracownicy są ostrzegani, żeby nie nadużywać tego systemu – na przykład poprzez wysuwanie fałszywych lub bezpodstawnych zarzutów wobec innych członków personelu. Otrzymują również wyjaśnienie, że mogą korzystać z systemu anonimowo, jeśli wolą takie rozwiązanie, albo mogą ujawnić swoją tożsamość, jeśli tego chcą. W tym ostatnim przypadku pracownicy są informowani o okolicznościach, w których identyfikujące ich informacje zostaną przekazane pracodawcy lub innym agencjom.

Gdyby system ten trzeba było utworzyć na mocy prawa UE lub prawa państwa członkowskiego UE, podstawą przetwarzania mógłby być art. 7 lit. c). Zagraniczne zobowiązania prawne nie kwalifikują się jako zobowiązanie prawne dla celów art. 7 lit. c), a zatem takie zobowiązanie nie mogłoby być podstawą legalności przetwarzania na mocy art. 7 lit. c). Przetwarzanie mogłoby jednak być oparte na art. 7 lit. f), gdyby na przykład istniał uzasadniony interes leżący w zapewnieniu stabilności rynków finansowych lub w walce z korupcją oraz pod warunkiem, że system ten obejmuje wystarczające gwarancje zgodnie z wytycznymi właściwych organów regulacyjnych w UE.

Przykład 16: „Wewnętrzny" system informowania o nieprawidłowościach bez spójnych procedur

Przedsiębiorstwo świadczące usługi finansowe postanawia utworzyć system informowania o nieprawidłowościach, ponieważ podejrzewa, że jego pracownicy powszechnie dopuszczają się kradzieży i korupcji, oraz pragnie ich zachęcić do donoszenia na siebie nawzajem. W celu zaoszczędzenia pieniędzy przedsiębiorstwo decyduje, że system ten będzie obsługiwany wewnętrznie, przez pracowników jego działu kadr. Aby zachęcić pracowników do korzystania z systemu, oferuje bez zadawania zbędnych pytań nagrody pieniężne dla pracowników, którzy poprzez zgłoszenie nieprawidłowości doprowadzili do wykrycia niedozwolonego postępowania i odzyskania pieniędzy.

Przedsiębiorstwo to ma uzasadniony interes leżący w wykrywaniu kradzieży i korupcji oraz zapobieganiu tym zjawiskom. Jego system informowania o nieprawidłowościach jest jednak tak źle zaprojektowany i pozbawiony gwarancji, że jego interesy są podrzędne w stosunku do interesów i prawa do prywatności jego pracowników – zwłaszcza tych, którzy mogą być ofiarą fałszywych doniesień złożonych wyłącznie dla korzyści finansowej. Fakt, że system ten obsługiwany jest wewnętrznie, a nie niezależnie, stanowi tu kolejny problem, podobnie jak brak szkolenia i wytycznych w zakresie korzystania z systemu.

Bezpieczeństwo fizyczne, bezpieczeństwo informatyczne i bezpieczeństwo sieci

Przykład 17: Kontrole biometryczne w laboratorium badawczym

W laboratorium, w którym prowadzone są badania naukowe nad śmiercionośnymi wirusami, ze względu na wysokie ryzyko dla zdrowia publicznego, jakie miałoby miejsce w przypadku wydostania się tych wirusów, wykorzystywany jest biometryczny system wejścia. Stosowane są odpowiednie gwarancje, w tym przechowywanie danych biometrycznych na osobistych kartach pracowniczych, a nie w systemie scentralizowanym.

Nawet jeżeli dane te są w ujęciu ogólnym danymi szczególnie chronionymi, powodem ich przetwarzania jest interes publiczny. To oraz fakt, że ryzyko nadużycia jest zmniejszone poprzez właściwe stosowanie gwarancji, sprawia, że art. 7 lit. f) jest odpowiednią podstawą przetwarzania.

Przykład 18: Ukryte kamery na potrzeby identyfikacji palących gości i pracowników

Przedsiębiorstwo korzysta z ukrytych kamer w celu identyfikacji pracowników i gości, którzy palą w budynku w miejscach niedozwolonych.

Podczas gdy administrator danych ma uzasadniony interes leżący w zapewnieniu zgodności z przepisami zabraniającymi palenia, środki użyte do osiągnięcia tego celu są – ogólnie rzecz biorąc – nieproporcjonalne i nadmiernie inwazyjne. Dostępne są metody mniej inwazyjne i bardziej przejrzyste (takie jak czujniki dymu i widoczne oznakowanie). Przetwarzanie to nie jest zatem zgodne z art. 6, który zawiera wymóg, żeby dane były „nienadmierne ilościowo” w stosunku do celów, dla których zostały zgromadzone lub dalej przetworzone. Jednocześnie przetwarzanie to prawdopodobnie nie spełni testu równowagi na mocy art. 7.

Badania naukowe

Przykład 19: Badania nad wpływem rozwodu i bezrobocia rodziców na wykształcenie dzieci

W ramach programu badawczego przyjętego przez rząd i zatwierdzonego przez właściwą komisję etyki przeprowadza się badania nad związkiem między rozwodem, bezrobociem rodziców a wykształceniem dzieci. Głównym przedmiotem badania są kwestie, które chociaż

nie zaliczają się do „szczególnych kategorii danych", byłyby jednak przez wiele rodzin uważane za bardzo intymne dane osobowe. Badania te pozwolą zapewnić specjalną pomoc edukacyjną dzieciom, które w przeciwnym razie mogłyby opuszczać zajęcia, zdobyć niższe wykształcenie, zostać dorosłymi bezrobotnymi i popełniać przestępstwa. Prawo danego państwa członkowskiego wyraźnie zezwala na przetwarzanie danych osobowych (innych niż szczególne kategorie danych) do celów badań naukowych, pod warunkiem że badania te są konieczne dla ważnych interesów publicznych i przeprowadzone z zachowaniem odpowiednich gwarancji, które są szczegółowo określone w przepisach wykonawczych. Te ramy prawne obejmują szczegółowe wymogi, ale również ramy rozliczalności, które umożliwiają przeprowadzenie indywidualnej oceny dopuszczalności badań (jeśli są prowadzone bez zgody zainteresowanych osób) i konkretnych środków, które należy stosować w celu ochrony osób, których dane dotyczą.

Naukowiec prowadzi te badania w bezpiecznej placówce badawczej, do której istotne informacje są dostarczane – z zachowaniem środków bezpieczeństwa – przez rejestr ewidencji ludności, sądy, agencje zatrudnienia i szkoły. W ośrodku badawczym następnie przeprowadza się anonimizację danych dotyczących tożsamości, tak aby można było powiązać dane dotyczące rozwodu, bezrobocia i wykształcenia, ale bez ujawniania tożsamości osób fizycznych, np. ich imion i nazwisk oraz adresów. Wszystkie oryginalne dane są następnie bezpowrotnie usuwane. Podejmowane są także dalsze środki służące zapewnieniu rozdziału funkcjonalnego (tj. wykorzystywaniu danych wyłącznie do celów badawczych) i zmniejszeniu jakiegokolwiek ryzyka ponownej identyfikacji.

Personel pracujący w tym ośrodku badawczym przechodzi rygorystyczne szkolenie w zakresie bezpieczeństwa i jest osobiście – być może nawet karnie – odpowiedzialny za wszelkie naruszenia bezpieczeństwa, za które odpowiada. Wprowadzane są środki techniczne i organizacyjne na przykład w celu zapewnienia, aby personel przy użyciu pamięci USB nie mógł wyprowadzić danych osobowych z ośrodka.

Prowadzenie tych badań leży w uzasadnionych interesach ośrodka badawczego i stanowi ważny interes publiczny. Leży również w uzasadnionych interesach organów do spraw zatrudnienia i edukacji oraz innych instytucji zaangażowanych w przedmiotową inicjatywę, ponieważ badania te pomogą im w planowaniu i świadczeniu usług na rzecz osób, które najbardziej ich potrzebują. Aspekty prywatności tej inicjatywy zostały dobrze zaprojektowane, a wprowadzone gwarancje oznaczają, że uzasadnione interesy organizacji zaangażowanych w prowadzenie badań nie są podrzędne względem interesów lub prawa do prywatności rodziców lub dzieci, których dane stanowiły podstawę badań.

Przykład 20: Badanie na temat otyłości

Uczelnia chce przeprowadzić badania nad poziomem otyłości u dzieci w wielu miastach i gminach wiejskich. Pomimo ogólnych trudności z uzyskaniem dostępu do odpowiednich danych ze szkół i innych instytucji udaje jej się przekonać kilkudziesięciu nauczycieli do monitorowania w swoich klasach przez pewien okres dzieci, które wydają się otyłe, i zadawania im pytań na temat diety, aktywności fizycznej, grania w gry komputerowe itd. Nauczyciele rejestrują również imiona i nazwiska oraz adresy dzieci, z którymi prowadzą rozmowy, żeby w nagrodę za udział w badaniu można było przesłać im kupon na zakup utworów muzycznych w Internecie. Badacze następnie kompilują bazę danych dzieci i korelują poziom otyłości z aktywnością fizyczną i innymi czynnikami. Papierowe wersje wypełnionych kwestionariuszy dotyczących rozmowy – nadal w formie, która pozwala na

zidentyfikowanie poszczególnych dzieci – są przechowywane w archiwach uczelni przez czas nieokreślony i bez odpowiednich środków bezpieczeństwa. Kserokopie wszystkich kwestionariuszy są udostępniane na żądanie każdemu magistrantowi lub doktorantowi, który wykazuje zainteresowanie dalszym wykorzystaniem tych danych, na tej uczelni oraz w partnerskich szkołach wyższych na całym świecie.

Chociaż prowadzenie badań naukowych leży w uzasadnionych interesach uczelni, istnieje kilka aspektów projektu tych badań, które powodują, że interesy te są podrzędne względem interesów i prawa do prywatności dzieci. Poza metodyką badań, której brakuje ścisłości naukowej, problemem jest zwłaszcza nieuwzględnienie w projekcie badań rozwiązań służących wzmocnieniu ochrony prywatności oraz szeroki dostęp do zgromadzonych danych osobowych. W żadnym momencie dane dzieci nie są kodowane ani poddawane anonimizacji. Nie podejmuje się też innych środków w celu zapewnienia bezpieczeństwa danych lub rozdziału funkcjonalnego. Nie uzyskuje się również ważnej zgody, o której mowa w art. 7 lit. a) i art. 8 ust. 2 lit. a), i nie jest jasne, czy dzieciom lub ich rodzicom wyjaśniono, do czego ich dane osobowe będą wykorzystywane lub komu będą udostępniane.

Zagraniczne zobowiązanie prawne

Przykład 21: Zgodność z wymogami prawa podatkowego państwa trzeciego

Banki w UE gromadzą i przekazują pewne dane swoich klientów na potrzeby spełnienia przez tych klientów obowiązków podatkowych wobec państw trzecich. Gromadzenie i przekazywanie danych jest przewidziane w umowie międzynarodowej pomiędzy UE a państwem trzecim określone i odbywa się w oparciu o uzgodnione przez nie w tej umowie warunki i gwarancje.

Podczas gdy zobowiązanie zagraniczne samo w sobie nie może być uznane za uzasadnioną podstawę przetwarzania na mocy art. 7 lit. c), może być jednak taką podstawą, jeżeli zobowiązanie takie jest uwzględnione w umowie międzynarodowej. W tym ostatnim przypadku przetwarzanie można byłoby uznać za konieczne dla wykonania zobowiązania prawnego włączonego w wewnętrzne ramy prawne na podstawie umowy międzynarodowej. Jeżeli jednak taka umowa nie istnieje, gromadzenie i przekazywanie danych trzeba będzie poddać ocenie w oparciu o wymogi określone w art. 7 lit. f) i można będzie uznać te czynności za dopuszczalne tylko pod warunkiem, że zapewnione są odpowiednie gwarancje, takie jak te zatwierdzone przez właściwy organ ochrony danych (zob. także *przykład 15* powyżej).

Przykład 22: Przekazywanie danych dotyczących dysydentów

Przedsiębiorstwo w UE na żądanie przekazuje dane zagranicznych rezydentów opartemu na ucisku reżimowi w państwie trzecim, który chce uzyskać dostęp do danych dotyczących dysydentów (np. danych o ruchu dotyczącym poczty elektronicznej, treści wiadomości e-mail, historii przeglądania lub prywatnych wiadomości w portalach społecznościowych).

W tym przypadku, w przeciwieństwie do poprzedniego przykładu, nie ma umowy międzynarodowej, która umożliwiłaby stosowanie art. 7 lit. c) jako podstawy prawnej. Poza tym kilka elementów przemawia przeciwko art. 7 lit. f) jako odpowiedniej podstawie przetwarzania. Chociaż administrator danych może mieć interes gospodarczy leżący w zaspokajaniu żądań zagranicznego rządu (w przeciwnym razie rząd państwa trzeciego mógłby

traktować administratora danych mniej korzystnie w porównaniu z innymi przedsiębiorstwami), legalność i proporcjonalność przekazywania danych jest bardzo wątpliwa, biorąc pod uwagę unijne ramy praw podstawowych. Potencjalnie ogromny wpływ przekazywania danych na zainteresowane osoby (np. dyskryminacja, pozbawienie wolności, kara śmierci) również zdecydowanie przemawia za interesami i prawami tych osób.

Ponowne wykorzystywanie publicznie dostępnych danych

Przykład 23: Ocena polityków[126]

Organizacja pozarządowa działająca na rzecz przejrzystości wykorzystuje publicznie dostępne dane dotyczące polityków (obietnice składane podczas wyborów oraz zapisy dotyczące faktycznego głosowania), aby oceniać ich na podstawie tego, jak wywiązują się ze swoich obietnic.

Nawet jeżeli wpływ na zainteresowanych polityków może być znaczny, fakt, że przetwarzanie jest oparte na informacjach publicznych oraz ma związek z obowiązkami publicznymi polityków, sprawia, że z uwagi na wyraźny cel polegający na zwiększeniu przejrzystości i rozliczalności przeważa interes administratora danych[127].

Dzieci i inne osoby wymagające szczególnego traktowania

Przykład 24: Strona informacyjna dla nastolatków

Na stronie internetowej organizacji pozarządowej, na której oferowane są porady dla nastolatków dotyczące takich kwestii, jak: narkomania, niechciana ciąża i nadużywanie alkoholu, za pomocą jej własnego serwera gromadzone są dane na temat osób odwiedzających te stronę. Następnie dane te są natychmiast poddawane anonimizacji i przekształcane w ogólne statystyki dotyczące tego, które części tej strony są najbardziej popularne wśród gości pochodzących z różnych regionów geograficznych danego państwa.

Artykuł 7 lit. f) mógłby być wykorzystany jako podstawa prawna nawet w odniesieniu do danych dotyczących osób wymagających szczególnego traktowania, ponieważ przetwarzanie leży w interesie publicznym i wprowadzone są surowe gwarancje (dane są natychmiast anonimizowane i wykorzystywane wyłącznie do tworzenia statystyk), co pomaga przechylić szalę na korzyść administratora danych.

Rozwiązania w zakresie uwzględnienia ochrony prywatności już w fazie projektowania jako dodatkowe gwarancje

Przykład 25: Dostęp do numerów telefonów komórkowych użytkowników aplikacji i osób niebędących jej użytkownikami: rozwiązanie „porównaj i zapomnij”

[126] Zob. i por. również przykład 7 powyżej.

[127] Podobnie jak w *przykładach 1 i 2* założono, że publikacja jest dokładna i proporcjonalna – brak gwarancji i inne czynniki mogą zmienić równowagę interesów w zależności od okoliczności danego przypadku.

Dane osobowe osób fizycznych są przetwarzane w celu sprawdzenia, czy osoby te w przeszłości udzieliły już jednoznacznej zgody (tj. rozwiązanie „porównaj i zapomnij" jako gwarancja).

Twórca aplikacji musi mieć jednoznaczną zgodę osób, których dane dotyczą, na przetwarzanie ich danych osobowych: na przykład twórca aplikacji chce mieć dostęp do całej elektronicznej książki adresowej użytkowników aplikacji, w tym numerów telefonów komórkowych osób, które są nie korzystają z tej aplikacji, i móc gromadzić te dane. Aby móc to zrobić, musi najpierw ocenić, czy właściciele numerów telefonów komórkowych figurujących w książkach adresowych użytkowników aplikacji udzielili jednoznacznej zgody (na mocy art. 7 lit. a)) na przetwarzanie ich danych.

W odniesieniu do tego ograniczonego przetwarzania wstępnego (tj. tymczasowego dostępu do odczytu pełnej książki adresowej użytkownika aplikacji) twórca aplikacji może powołać się na art. 7 lit. f) jako podstawę prawną, z zastrzeżeniem gwarancji. Gwarancje te powinny obejmować środki techniczne i organizacyjne służące zapewnieniu, aby przedsiębiorstwo wykorzystywało ten dostęp tylko po to, żeby pomóc użytkownikowi określić, które osoby figurujące w jego książce adresowej są już użytkownikami, a zatem już udzieliły temu przedsiębiorstwu w przeszłości jednoznacznej zgody na gromadzenie i przetwarzanie numerów telefonicznych w tym celu. Numery telefonów komórkowych osób niebędących użytkownikami aplikacji mogą być gromadzone i wykorzystywane wyłącznie na potrzeby ściśle ograniczonego celu polegającego na sprawdzeniu, czy osoby te wyraziły jednoznaczną zgodę na przetwarzanie ich danych, i po tej czynności numery te należy niezwłocznie usunąć.

Łączenie danych osobowych w ramach wielu usług internetowych

Przykład 26: Łączenie danych osobowych w ramach wielu usług internetowych

Przedsiębiorstwo internetowe świadczące różne usługi, w tym usługi wyszukiwarki, udostępniania treści wideo i sieci społecznościowej, opracowuje politykę prywatności, która zawiera klauzulę umożliwiającą mu „łączenie wszystkich danych osobowych" zgromadzonych na temat wszystkich użytkowników w odniesieniu do różnych usług, z których korzystają, bez określenia okresu zatrzymywania danych. Według przedsiębiorstwa odbywa się to w celu „zagwarantowania jak najlepszej jakości usług".

Przedsiębiorstwo udostępnia pewne narzędzia różnym kategoriom użytkowników, aby mogli oni korzystać ze swoich praw (np. wyłączyć ukierunkowane reklamy, sprzeciwić się pobieraniu określonego typu plików cookie).

Dostępne narzędzia nie pozwalają jednak użytkownikom na skuteczne kontrolowanie przetwarzania ich danych: użytkownicy nie mogą kontrolować konkretnych kombinacji swoich danych w ramach różnych usług i nie mogą wyrazić sprzeciwu wobec łączenia danych na swój temat. Ogólnie rzecz biorąc, nie ma równowagi między uzasadnionym interesem przedsiębiorstwa a ochroną praw podstawowych użytkowników i art. 7 lit. f) nie należy przywoływać jako podstawy prawnej przetwarzania. Artykuł 7 lit. a) stanowiłby odpowiedniejszą podstawę, pod warunkiem że spełnione są warunki dotyczące ważnej zgody.