



1806/16/EN
WP 239

**Opinia 2/2016 dotycząca publikacji danych osobowych dla celów przejrzystości
w sektorze publicznym**

Przyjęta w dniu 8 czerwca 2016 r.

Grupa Robocza została ustanowiona na podstawie art. 29 Dyrektywy 95/46/WE. Jest ona niezależnym organem doradczym w sprawie ochrony danych oraz prywatności. Jej zadania są opisane w art. 30 Dyrektywy 95/46/WE oraz art. 15 Dyrektywy 2002/58/WE.

Sekretariat jest zapewniony przez Dyрекję C (Prawa podstawowe oraz obywatelstwo Unii) Komisji Europejskiej, Dyrekcja Generalna ds. Sprawiedliwości oraz Konsumentów, B-1049 Bruksela, Belgia, numer biura MO-59 02/013.

Adres strony internetowej: http://ec.europa.eu/justice/data-protection/index_en.htm

WSTĘP

1.1 ZAKRES OPINII

Niniejsza opinia wyjaśnia w jaki sposób stosować zasady ochrony danych w odniesieniu do przetwarzania oraz publikacji danych osobowych dla celów przejrzystości w sektorze publicznym, w szczególności w odniesieniu do środków antykorupcyjnych oraz zarządzania oraz zapobiegania konfliktom interesów¹. Celem niniejszej opinii nie jest próba ustalenia tego jakie informacje powinny być dostępne na podstawie przepisów krajowych dotyczących dostępu do dokumentów publicznych/ wolności wypowiedzi w państwach członkowskich UE², nie ogranicza ona również dostępności takich informacji publicznych zgodnie z prawodawstwem krajowym, jak również nie obejmuje wdrożenia Rozporządzenia 45/2001 oraz Rozporządzenia 1049/2001³, właściwych w odniesieniu do instytucji oraz organów Unii Europejskiej.

Ogólnie rzecz ujmując, w odniesieniu do podmiotów sektora publicznego może istnieć wymóg zbierania, utrwalania oraz przechowywania informacji o działalności ich oraz ich pracowników, w celu upublicznienia tych informacji, zwykle za pomocą ich oficjalnych stron internetowych. Prawdopodobnym jest, że taki sposób przetwarzania będzie obejmował przetwarzanie danych osobowych, obejmujące rozpowszechnianie takich informacji wśród opinii publicznej.

Niniejsza opinia skierowana jest do krajowych instytucji prawodawczych, rządów krajowych, urzędów, agencji oraz innych właściwych instytucji („instytucje właściwe”) w sektorze publicznym, które zajmują się zwalczaniem korupcji, środkami przeciwdziałania konfliktom interesów oraz innymi zobowiązaniami w zakresie przejrzystości, jak również do organów ochrony danych. Zalecenia zostały sformułowane na podstawie wspólnego rozumienia ram ochrony danych, w ramach których takie przetwarzanie ma miejsce. W szczególności dotyczy ona ogólnych kwestii związanych z wdrożeniem zasad oraz wartości Dyrektywy 95/46/WE⁴ oraz Ogólnego rozporządzenia o ochronie danych (dalej Ogólne rozporządzenie).

¹ Sektor publiczny – dla celów niniejszej Opinii, sektor publiczny oznacza instytucje państwowe, regionalne lub lokalne, podmioty działające na podstawie prawa publicznego oraz zrzeszenia utworzone z udziałem jednej lub kilku takich instytucji, lub jednej lub kilku podmiotów, działających na podstawie prawa publicznego. Definicja ta pozostaje bez uszczerbku dla definicje ustanowionych w przepisach państw członkowskich.

² Zobacz Opinię GR29 06/2013 w sprawie otwartych zbiorów danych oraz informacji sektora publicznego.

³ 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 oraz Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji.

⁴ 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

Artykuły 1 oraz 2 Dyrektywy 95/46/WE wymagają, aby państwa członkowskie zobowiązały się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych. Państwa członkowskie zobowiązują się również, że przetwarzanie danych osobowych w ramach środków antykorupcyjnych nakierowanych na rozwiązywanie potencjalnych konfliktów interesów oraz jakichkolwiek innych obowiązków związanych z przejrzystością, są regulowane przez przepisy krajowe, przyjęte przez nie na podstawie dyrektywy oraz w świetle Ogólnego rozporządzenia.

1.2 CEL OPINII

Celem niniejsze opinii jest zapewnienie praktycznych wytycznych, zaleceń oraz przykładów najlepszych praktyk dla prawodawców oraz właściwych instytucji państw członkowskich, odnośnie tego w jaki sposób mogą one zapewnić, że prawo do ochrony danych osobowych jest przestrzegane, jednocześnie równoważąc oraz zapewniając poszanowanie uzasadnionego interesu publicznego przejrzystości, w przypadkach gdy inicjatywy legislacyjne oraz polityczne w takich kwestiach, wymagają ujawnienia informacji o osobach fizycznych. Pojęcie „przejrzystości”⁵ łączy się z zasadami jawności, dobrej administracji oraz dobrego zarządzania, jak to wskazano w Traktatach⁶ oraz Karcie praw podstawowych Unii Europejskiej (Karcie UE)⁷.

Bezstronność, przejrzystość oraz profesjonalne zachowanie osób z sektora z publicznego jest uznawane za kluczowe, w zapewnianiu doskonałości oraz jakości wypełniania zadań na określonych stanowiskach publicznych. Należy osiągnąć równowagę pomiędzy prawem ochrony danych⁸ osób z sektora publicznego z jednej strony oraz interesu publicznego, polegającego na zapewnieniu przejrzystości wykonywania swoich obowiązków przez te osoby z drugiej. Publikowanie szczegółów dotyczących interesów prywatnych osób z sektora publicznego jest jednym z szeregu środków, wykorzystywanych do rozwiązywania potencjalnych konfliktów interesów oraz zwiększania rozliczalności oraz zaufania publicznego. Chociaż prawa dotyczące rozwiązywania konfliktów interesów różnią się, niniejsza opinia doradza w kwestii tego, w jaki sposób zapewnić równy poziom ochrony danych osób z sektora publicznego w różnych państwach członkowskich.

⁵ Odniesienie to pozostaje bez uszczerbku dla szczegółowych definicji określonych w prawie krajowym oraz politykach a dodano je jedynie w celu uczynienia niniejszej opinii bardziej zrozumiałą. .

⁶ Zobacz art. 10 oraz 11 Traktatu o Unii Europejskiej oraz art. 15 oraz 298 Traktatu o Funkcjonowaniu Unii Europejskiej.

⁷ Zobacz art. 41 Karty UE.

⁸ Prawo ochrony danych musi być rozumiane jako prawo do ochrony na mocy Dyrektywy 95/46/WE oraz Ogólnego rozporządzenia.

2. RAMY PRAWNE

Artykuł 7 Karty UE stanowi, że każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się. Dodatkowo, art. 8 Karty przewiduje, między innymi, że każdy ma prawo do ochrony danych osobowych, które go dotyczą. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Również artykuł 8 Europejskiej Konwencji Praw Człowieka (EKPCz) stanowi, że Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji oraz, że niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób.

Artykuł 7 Dyrektywy 95/46/WE zawiera kryteria legalności przetwarzania danych osobowych oraz ustanawia podstawowe zasady przetwarzania danych osobowych (art. 6 Dyrektywy 95/46). Motywy Ogólnego rozporządzenia precyzują, że Dyrektywa 2003/98/WE Parlamentu Europejskiego oraz Rady z dnia 17 listopada 2003 w sprawie ponownego wykorzystania informacji sektora publicznego nie narusza ani w żaden stopień nie wpływa na stopień ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, wynikający z prawa Unii lub prawa państw członkowskich.

Zgodnie z art. 10 EKPCz każdy ma prawo do wyrażania opinii. ETPCz wielokrotnie rozpoznał, że prawo to obejmuje „prawo opinii publicznej do odpowiedniej informacji” oraz „prawo do uzyskania informacji” nie tylko w przypadkach dotyczących mediów oraz zawodowych dziennikarzy⁹.

W świetle powyższych przepisów zaleca się, aby wziąć pod uwagę następujące zasady, w przypadku przetwarzania danych osobowych w sytuacji środków przeciwdziałania konfliktowi interesów oraz wiążącej się z tym przejrzystości

⁹ Jednakże do niedawna, ETPCz stał na stanowisku, że wolność uzyskania informacji, zagwarantowana w art. 10, nie może być rozumiana jako pozytywny obowiązek nakładany na państwo, rozwposzechnienia lub ujawnienia informacji opinii publicznej (zobacz sprawy Leander przeciwko Szwecji (1987), Gaskin przeciwko Zjednoczone Królestwo (1989), Guerra przeciwko Włochom (1998) oraz Sirbu przeciwko Mołdawii (2004)). Wydaje się, że jedynie w dwóch ostatnich sprawach Sąd skłonił się ku szerszej interpretacji pojęcia wolności informacji (zobacz decyzja z 2006 r. dotycząca dopuszczenia wbujsy w sorawue Sdružení Jihočeské Matky przeciwko Republika Czeska oraz decyzję z 2009 r. w sprawie Társaság a Szabadságjogokért przeciwko Węgry).

3. ZASADY OCHRONY DANYCH OSOBOWYCH

Art. 6 Dyrektywy 95/46/WE stanowi, że dane osobowe muszą być:

- a) przetwarzane rzetelnie i legalnie;
- b) gromadzone do określonych, jednoznacznych i legalnych celów oraz nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem.
- c) prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone;
- d) prawidłowe oraz, w razie konieczności, aktualizowane;
- e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane.

Powyższe wymogi pozostają w zgodności z równoważnymi przepisami Ogólnego rozporządzenia.

3.1 RZETELNE ORAZ LEGALNE PRZETWARZANIE

Podstawę prawną przetwarzania danych osobowych w kontekście środków przeciwdziałania konfliktowi interesów można znaleźć w art. 7 lit. c) Dyrektywy 95/46/WE¹⁰. Stanowi on, że dane osobowe mogą być przetwarzane jeżeli przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega. W takim przypadku przetwarzanie musi być wymagane przez prawo.¹¹ Wymaga to, aby przepis prawny był wystarczająco dokładny, wyraźnie określając jakie dane muszą być zbierane oraz/lub rozpowszechniane oraz dla jakiego celu. W związku z tym, należy unikać wprowadzenia ogólnych, blankietowych przepisów, tak aby administrator nie posiadał niewłaściwego stopnia dowolności w odniesieniu do tego w jaki sposób zapewnić zgodność z obowiązkiem prawnym¹².

W takich okolicznościach, prawodawcy mają obowiązek zapewnienia, aby zobowiązania prawne równoważyły różne zaangażowane interesy. Prawodawstwo musi być zgodne z prawem do prywatności oraz życia rodzinnego oraz ochrony danych osobowych zgodnie z art. 8 EKPCz oraz artykułami 7 oraz 8 Karty UE¹³. Oznacza to, że zobowiązanie prawne przetwarzania danych osobowych powinno być konieczne oraz proporcjonalne względem uzasadnionych celów, do których dąży administrator danych oraz zgodne z zasadą ograniczenia celu.

Instytucje mogą również polegać na artykule 7 e) dyrektywy, jako na podstawie przetwarzania danych osobowych w tym kontekście. Przy określaniu czy operacje przetwarzania są zgodne z art. 7 lit. e) oraz mając na uwadze różne zaangażowane interesy, instytucje muszą być przekonane, że:

¹⁰ W celu uzyskania bardziej szczegółowej analizy zobacz Opinię 06/2014 w sprawie pojęcia uzasadnionego interesu administratora danych na podstawie art. 7 Dyrektywy 95/46/WE, WP217. W niektórych krajach może być możliwe oparcie się na art. 7 litera f) jako na podstawie przetwarzania takiego rodzaju danych osobowych.

¹¹ W opinii 06/2014 GR29 uznała, że aby art. 7 litera c) znajdował zastosowanie, obowiązek musi być nałożony przez prawo, które spełnia wszystkie odpowiednie warunki, aby zobowiązanie było wiążące. W tym aspekcie GR29 zauważyła, że „prawo w niektórych sytuacjach może ustanawiać jedynie ogólny cel, podczas gdy bardziej szczegółowe obowiązki mogą być nałożone na innym poziomie, na przykład w prawie wykonawczym lub we wiążących decyzjach władz publicznych w konkretnym przypadku“. W tym kontekście Ogólne rozporządzenie wyjaśnia, że „w przypadku gdy w niniejszym rozporządzeniu jest mowa o podstawie prawnej lub akcie prawnym, niekoniecznie wymaga to przyjęcia aktu prawnego przez parlament, z zastrzeżeniem wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego“. Zobacz również art. 6 ustęp 3 Ogólnego rozporządzenia.

¹² Tamże.

¹³ Zobacz wyrok TSUE z dnia 20 maja 2003 w połączonych sprawach C-465/00, C-138/01 oraz C-139/01 Rundfunk oraz z dnia 9 listopada 2010 w połączonych sprawach C-92/09 oraz C-93/09 Volker und Markus Schecke.

- operacja przetwarzania jest zadaniem wykonywanym w interesie publicznym lub dla wykonywania władzy publicznej¹⁴;
- przetwarzanie jest niezbędne dla wykonania tego zadania lub dla wykonywania władzy publicznej (oznacza to, że takie operacje muszą być odpowiednie dla osiągnięcia zamierzonego celu oraz nie mogą wykroczyć poza to co jest konieczne dla jego osiągnięcia).

Przykład: Indeksowanie¹⁵ danych osobowych wprowadzonych do platform przejrzystości, w celu umożliwienia obywatelom dokonywania wyszukiwania, byłoby uznane za konieczną operację. Indeksacja danych dotyczących tożsamości dla zewnętrznej wyszukiwarki nie byłoby uznana za konieczną, co do zasady, dla osiągnięcia celu przejrzystości.

3.2 ZASADY PROPORCJONALNOŚCI, MINIMALIZACJI ORAZ JAKOŚCI DANYCH

W celu wdrożenia tych zasad, przede wszystkim koniecznym jest określenie głównych celów przetwarzania danych. Na przykład, inicjatywy w obszarze przejrzystości mogą mieć za zadanie zwiększanie szeroko rozpowszechnianej wiedzy o decyzjach oraz działaniach rządu oraz organów administracyjnych, oferując podstawowy wgląd w procesy, działania oraz pracowników. W konsekwencji, pozwala to opinii publicznej pociągać do odpowiedzialności rząd za to w jaki sposób wykonuje swoje zadania oraz zarządza zasobami publicznymi, promując w ten sposób wydajność oraz skuteczność. Środki, których dotyczy niniejsza opinia mają za cel zapobieganie, wykrywanie oraz karanie konfliktów interesów, mając na uwadze unikanie wpływu interesów prywatnych na wykonywanie obowiązków publicznych oraz wzmocnienie uczciwości, obiektywności, bezstronności osób z sektora publicznego, jak również budowanie zaufania obywateli do rządu.

PRZYKŁAD: Zadaniem odpowiednich instytucji jest określenie wartości aktywów, które posiadały osoby z sektora publicznego w momencie objęcia oraz opuszczenia stanowiska oraz zidentyfikowanie w jaki sposób aktywa te były finansowe. Aby to osiągnąć, konieczne może być zebranie informacji na temat małżonków oraz krewnych oraz ich aktywów. Nie oznacza to jednak koniecznie, że odpowiednim oraz proporcjonalnym jest udostępnianie tych wszystkich danych publicznie przez Internet. Jakiegokolwiek naruszenie prywatności osób fizycznych powinno być konieczne oraz proporcjonalne wobec uzasadnionego celu przetwarzania.

¹⁴ Jak podkreśliła GR29 w opinii 6/2014, zadanie publiczne lub władza publiczna powinna się opierać lub wynikać z przepisów prawa. Zobacz Część II, ust. 2.5, jak również motyw 41 oraz art. 6 ust. 3 Ogólnego rozporządzenia.

¹⁵ Definicja indeksowania :

3.2.1 PROPORCJONALNOŚĆ

Zasada proporcjonalności powinna być przestrzegana w odniesieniu do każdej operacji przetwarzania, w szczególności na etapie zbierania oraz późniejszej publikacji.

Trybunał Sprawiedliwości Unii Europejskiej (dalej TS UE) podkreślił znaczenie podejścia opartego na proporcjonalności w odniesieniu do przetwarzania danych osobowych przy kilku okazjach. We wspomnianych już połączonych sprawach C-465/00, C-138/01 oraz C-139/01, TS UE odniósł się do tego problemu, zadając pytanie: „czy wskazanie nazwisk danych osób w związku z pobranymi przez nie dochodami jest proporcjonalne do zamierzonego zasadnego celu oraz czy powody przywołane przed Trybunałem w celu uzasadnienia takiego ujawnienia są istotne i wystarczające” (punkt 86), oraz podkreślił, że właściwy sąd krajowy powinien zbadać czy *“czy publikacja taka jest zarazem konieczna i proporcjonalna względem celu (...) oraz w szczególności, czy taki cel nie może zostać równie skutecznie osiągnięty przez przekazanie imiennych informacji jedynie organom kontrolnym”* (punkt 88). Ponadto TS UE zapytał czy możliwe byłoby zastosowanie innych sposobów osiągnięcia uzasadnionego celu, co do których istniało prawdopodobieństwo, że naruszyłyby prywatność w mniejszym stopniu¹⁶.

Co więcej, w punkcie 74 wspomnianego już wyroku w połączonych sprawach C-92/09 oraz C-93/09, TS UE jasno stwierdził, że *„z utrwalonego orzecznictwa wynika, że zasada proporcjonalności, która zalicza się do podstawowych zasad prawa wspólnotowego, wymaga, by środki wprowadzone aktem Unii były odpowiednie do realizacji zamierzonego celu i nie wykraczały poza to, co jest konieczne do jego osiągnięcia (wyrok z dnia 8 czerwca 2010 r. w sprawie C-58/08 Vodafone i in., Zb.Orz. s. I-4999, pkt 51 i przytoczone tam orzecznictwo).”*

Państwa członkowskie powinny uważnie rozważyć zakres osób, które podlegają środkom związanym z przeciwdziałaniem konfliktowi interesów oraz przejrzystością. Przy określaniu tego, czyje dane będą przetwarzane, państwa członkowskie mogą zechcieć sporządzić odpowiednie, obiektywne kryteria, takie jak władza publiczna danej osoby, możliwość wydania lub alokacji pieniędzy publicznych, wynagrodzenie, okres kadencji, otrzymane dodatki, itp., mając na uwadze, że przetwarzanie nie powinno wykraczać poza to, co jest *„konieczne dla realizacji zasadnie zamierzonych celów, mając na względzie w szczególności powodowane przez taką publikację naruszenie praw przyznanych w art. 7 i 8 karty”*¹⁷.

Publikacja w Internecie informacji, które ujawniają nie mające znaczenia aspekty życia prywatnego osób nie są uzasadnione w świetle zasad rzetelności oraz proporcjonalności.

¹⁶ W tym aspekcie TS UE zapytał czy: „nie byłoby wystarczająco poinformowanie opinii publicznej jedynie odnośnie wynagrodzenia oraz innych korzyści finansowych”. Zobacz punkt 88 decyzji Sądu w połączonych sprawach C-465/00 oraz C-138/01 Rundfunk.

¹⁷ TS UE wypowiedział się w wyrokach w połączonych sprawach Volker und Markus Schecke GbR (C-92/09) oraz Hartmut Eifert (C-93/09) przeciwko Land Hessen, punkty 79 oraz 80.

❖ Wdrażanie proporcjonalności:

➤ *Różnice pomiędzy zbieraniem a publikowaniem danych w Internecie*

Środki dotyczące konfliktu interesów pokrywają w ogólności dwie główne czynności przetwarzania: wyłącznie niepubliczne przetwarzanie danych osobowych przez właściwe instytucje oraz publikowanie niektórych danych w Internecie. Odpowiednie przepisy prawa powinny wyraźnie stanowić, które osoby są zobowiązane do składania sprawozdań właściwym instytucjom. Powinny również określić, które dane osobowe sprawozdania mają zawierać oraz które dane osobowe powinny być pro aktywnie publikowane. Niniejsza opinia nie próbuje określić, jakie dane osobowe powinny być zbierane przez odpowiednie instytucje zajmujące się środkami dotyczącymi konfliktów interesów, ani nie ma zamiaru określić, które dane powinny być rozpowszechniane przez Internet. Jednakże właściwym jest podkreślenie, że w przypadku decydowania czy ujawnić informacje w Internecie, właściwe instytucje powinny zawsze pamiętać o konsekwencjach takiego działania. Niektóre zbierane dane osobowe mogą stanowić informację intymną o osobach z sektora publicznego i w związku z tym jej publikacja w Internecie może mieć poważne skutki dla ich praw do życia prywatnego oraz ochrony danych. Należy również zauważyć, że to co interesuje opinię publiczną nie jest tym samym co interes publiczny.

W ogólności, prawdopodobne jest, że ilość danych osobowych publikowanych przez Internet powinna być bardziej ograniczona, niż ta przekazywana instytucjom, gdyż prawdopodobnym jest, że pro aktywne ujawnienie niektórych informacji może być nieproporcjonalne, biorąc pod uwagę prawdopodobny wpływ publikacji na osoby, których dane dotyczą. Co więcej, niektóre informacje, które nie są pro aktywnie publikowane, mogą być ujawnione, gdy legislacja dotycząca dostępu do informacji znajduje zastosowanie zgodnie z ustawą oraz/lub z innymi odpowiednimi przepisami lub na wniosek sądu wymagającego ujawnienia. Przy ocenie czy uzyskanie oraz/lub opublikowanie danych osobowych osób z sektora publicznego jest konieczne, należy wziąć pod uwagę czy sprawy oraz/lub transakcje osób z sektora publicznego (finansowe, umowne lub inne) mają miejsce przed objęciem przez nich urzędu, kiedy były osobami prywatnymi bez mandatu publicznego. Właściwe instytucje nie mają zakazu zbierania tych danych na tej podstawie, w szczególności gdy podejmowane są działania budzące podejrzenia. Jednakże automatyczne publikowanie w Internecie wszystkich spraw/transakcji osób z sektora publicznego z okresu przed objęciem urzędu, możliwe do przeszukiwania za pomocą nazwiska oraz zawierające wszystkie szczegóły bez rozróżnienia w zależności od ich charakteru, rodzaju oraz zakresu może wykraczać poza to, co jest konieczne do osiągnięcia uzasadnionych celów.

Przy rozważaniu opublikowania danych osobowych w Internecie koniecznym jest rozważenie możliwego ryzyka takiego ujawnienia. Jeżeli przewidywane jest rutynowe lub obszerne publikowanie, silnie zaleca się ocenę wpływu na prywatność. Powinno się również rozważyć inne sposoby ujawnienia pewnych szczegółów osobistych, takie jak podsumowanie lub zestawienie w zagregowanej formie, w której osoby nie mogą być zidentyfikowane.

Właściwym jest również rozważenie czy charakter oraz zakres danych osobowych będących przedmiotem publikacji może powodować inne ryzyko, niż to dotyczące ochrony danych. Na przykład, publikowanie danych osobowych dotyczących sytuacji finansowej osoby, której dane dotyczą może uczynić ją podatną na działalność przestępców. Nie wyklucza to ujawnienia tych danych odpowiednim instytucjom, zajmującym się zbieraniem oraz przetwarzaniem takich danych.

Również przy publikowaniu informacji dotyczących umów oraz/lub podobnych stosunków osób z sektora publicznego, odpowiednie instytucje powinny być świadome, że niektóre dane mogą być objęte tajemnicą (handlową, bankową, zawodową lub inną). W takich przypadkach, koniecznym może być wyważenie praw do ochrony danych osobowych, ochrony tajemnicy oraz interesu publicznego w dostępie do tych informacji.

PRZYKŁAD: Dane osobowe członków gospodarstwa domowego lub członków rodziny osób z sektora publicznego, takie jak nazwiska, dane kontaktowe, adresy, itp. mogą być zbierane przez właściwe instytucje w celu wykonania ich obowiązków w tym obszarze; jednakże publikacja wszystkich takich informacji w Internecie może nie być proporcjonalna, chociaż każdy przypadek powinien być oceniany osobno.

➤ *Czynności przetwarzania w odniesieniu do różnych grup osób*

Należy przyjmować selektywne podejście do przetwarzania danych osobowych, rozróżniając różne grupy osób, spraw oraz celów, a także brać pod uwagę szczególne sytuacje w których treść szczegółowych danych jest publikowana. Należy wykorzystywać różne sposoby udostępniania informacji, w zależności od tego który jest odpowiedni.

Oceniając czy przetwarzania powinno obejmować publiczne rozpowszechnianie danych osobowych poprzez publikację w Internecie, różne sytuacje powinny być rozpatrywane w odmienny sposób. Właściwe instytucje mogą zechcieć wziąć pod uwagę stopień, w którym instytucja publiczna lub osoba z sektora publicznego jest wystawiona na ryzyko korupcji lub sytuacji konfliktu interesów; zakres działań lub zadań, które mają być wypełniane w interesie publicznym oraz wysokość funduszy publicznych, którymi zarządzają te osoby. Ujmując rzecz ogólnie, właściwym może być czynienie rozróżnienia w zależności od miejsca w hierarchii oraz odpowiedzialności za podejmowanie decyzji pomiędzy politykami, osobami pełniącymi wyższe funkcje w administracji lub innymi osobami publicznymi piastującymi urzędy, z którymi wiąże się odpowiedzialność polityczna; osoby „piastujące zwykłe stanowiska związane z zarządzaniem w sektorze publicznym”, które nie piastują stanowisk pochodzących z wyboru a jedynie zajmują stanowiska związane z zarządzaniem oraz „zwykłymi osobami z sektora publicznego”, które nie ponoszą samodzielnej odpowiedzialności za decyzje.

W tym kontekście, podczas gdy w odniesieniu do pierwszej grupy rozpowszechnianie danych osobowych za pomocą strony internetowej właściwej instytucji może być uznane za

proporcjonalne, to samo rozwiązanie może nie mieć zastosowania w odniesieniu do drugiej oraz trzeciej grupy. W odniesieniu do drugiej grupy, nazwiska oraz stanowiska mogą być publicznie dostępne, natomiast dane osobowe dotyczące pracowników nie byłyby publikowane (nawet jeżeli dotyczyłoby to jedynie danych osobowych dotyczących ich działań jako osób z sektora publicznego lub dotyczących ich działalności zawodowej¹⁸). Pozostaje to bez uszczerbku dla dostępności tych danych na podstawie zasad krajowych dotyczących publicznego dostępu do dokumentów.

Zaleca się czynienie rozróżnienia pomiędzy różnymi grupami osób z sektora publicznego, pracowników administracji oraz innych osób, podlegających tym przepisom szczególnym, w zależności od wspomnianych wyżej kryteriów oraz określenie różnych poziomów obowiązków dotyczących składania informacji odpowiednim instytucjom, w oparciu o to rozróżnienie. Prawodawca powinien pamiętać o tym rozróżnieniu, w szczególności w odniesieniu do jakichkolwiek obowiązków związanych z publikowaniem w Internecie.

Takie podejście ułatwiłoby dostarczanie różnych ilości oraz rodzajów danych osobowych w zależności od grupy osób i z tego względu pomogłoby w wypełnieniu wymogów zasady proporcjonalności, zgodnie z którą przetwarzanie danych osobowych może obejmować jedynie minimalną ilość danych, koniecznych do osiągnięcia uzasadnionego celu (wykrywanie oraz karanie konfliktu interesów).

PRZYKŁAD: Publikacja danych osobowych dotyczących składania oświadczeń dotyczących konfliktów interesów w odniesieniu do osób z sektora publicznego wykonujących zadania obejmujące jedynie odpowiedzialność administracyjną zostały uznane w niektórych sytuacjach za nieproporcjonalne, biorąc pod uwagę, że nie piastują one stanowisk pochodzących z wyboru lub ministerialnych. W odróżnieniu od powyższej sytuacji, deponowanie tych dokumentów we właściwych instytucjach kontrolnych zostało uznane za uzasadnione, mając na uwadze cel jakim jest wzmacnianie uczciwości oraz bezstronności tych osób oraz zapobieganie, wykrywanie oraz karanie sytuacji w których występuje konflikt interesów¹⁹.

3.2.2 ZASADA MINIMALIZACJI DANYCH

W odniesieniu do zasady minimalizacji, powinno się stosować ścisłą ocenę konieczności oraz proporcjonalności przetwarzanych danych (art. 6 Dyrektywy 95/46/WE oraz przepisy Ogólnego rozporządzenia). Ilość oraz rodzaj przetwarzanych danych osobowych musi być jasno określony. Jeżeli istnieje potrzeba przetwarzania danych osobowych, dane takie muszą

¹⁸ W tym kontekście, w połączonych sprawach C-465/00, C-138/01, TS UE zwrócił uwagę na orzecznictwo ETPCz odnośnie zakresu wyrażenia „życie prywatne” stwierdzając, że „nie może być ono interpretowane restrykcyjnie” oraz „nie ma ogólnej zasady uzasadniającej wykluczenie działań o charakterze zawodowym z zakresu pojęcia „życia prywatnego”. Zobacz punkt 79 decyzji Sądu.

¹⁹ Zobacz Conseil constitutionnel de la République Française, Décision n ° 2013-675 DC of 10.09.2013 concerning the "Loi organique relative à la transparence de la vie publique" (Projet de loi adopté le 17 septembre 2013 - TA No. 209)

być adekwatne, odpowiednie oraz nie nadmierne w odniesieniu do określonych celów, w zgodności z prawem, a jakakolwiek informacja, która nie jest konieczna do osiągnięcia tych celów nie powinna być w jakikolwiek sposób przetwarzana. Przetwarzanie danych osobowych przy wdrażaniu środków dotyczących konfliktów interesów oraz przejrzystości powinno skupiać się na celu, oraz być wobec niego odpowiednie, tak aby uniknąć niepotrzebnego przetwarzania. Jest prawdopodobnym, że takie postępowanie zwiększy skuteczność oraz wydajność przetwarzanych danych.

Publikacja w Internecie nie zawsze musi być konieczna do osiągnięcia celu przetwarzania; w niektórych przypadkach, dostarczenie ogólnych podstawowych informacji na temat poszczególnych obszarów działalności rządu lub sprawozdania z decyzji oraz czynności podejmowanych w sektorze publicznym w formie wskaźników może być wystarczające. Bardziej szczegółowe dane mogą być przekazane właściwym instytucjom nadzorczym pozwalając, gdy to konieczne, na publikacje w Internecie, lub udostępnienie publiczne tych danych na podstawie krajowych reguł dostępu do dokumentów publicznych.

PRZYKŁAD: Jeżeli konieczne jest zbieranie oraz publikowanie informacji na temat aktywów osób powiązanych z osobami sektora publicznego w Internecie (takich jak partnerzy, dzieci oraz inni członkowie rodziny lub członkowie gospodarstwa domowego), należy zwrócić uwagę na zasadę minimalizacji danych, poprzez rozważenie czy aktywa członków rodziny nie powinny być opublikowane w zdezagregowanej formie lub ograniczone jedynie do ogólnej wartości aktywów. Zakres w którym konieczna jest publikacja tożsamości wszystkich członków rodziny lub członków gospodarstwa domowego aby osiągnąć cel, również powinna być rozważona.

PRZYKŁAD: Niektóre krajowe reguły dotyczące przejrzystości przewidują publikację w Internecie informacji dotyczących wielkości dochodu jednostek oraz wynagrodzenia otrzymywanego przez osoby wykonujących zadania administracyjne wysokiego szczebla (np. osoby piastujące wyższe stanowiska w administracji). Generalnie aby zapewnić zgodność z takimi obowiązkami, zgodnie z zasadą minimalizacji danych, wystarczające może być opublikowanie całkowitej kwoty pieniędzy otrzymanej przez jednostki. Jednakże mało prawdopodobnym jest uznanie za proporcjonalne publikowania danych takich jak numer identyfikacji podatkowej, całe sprawozdania finansowe, szczegółowe dane uzyskane z dokumentów dotyczących zwrotu podatków lub dokumentów potwierdzających wypłatę, szczegółów bankowych lub adresów domowych, osobistych numerów telefonów lub prywatnych adresów poczty elektronicznej.

PRZYKŁAD: Jeżeli dochodzi do sytuacji w której opublikowane mają być dane finansowe jednostek (tj. długi, kredyty itp.), zaleca się, zgodnie z zasadą minimalizacji – publikację jedynie koniecznych oraz/lub podstawowych informacji, mając na uwadze wrażliwość tych danych oraz potencjalne ryzyko wynikające z takiej publikacji w Internecie. Z tego względu

zaleca się, aby prawo określało szczegóły publikacji, gdy ma miejsce publikacja danych finansowych w Internecie, w celu uniknięcia możliwych naruszeń lub nadmiernej publikacji tych danych w Internecie, które mogą wykroczyć poza uzasadniony oraz /lub zgodny z prawem cel, mając również na uwadze interes publiczny.

❖ Rodzaj danych

Przy przetwarzaniu danych osobowych w ramach środków związanych z konfliktem interesów oraz przejrzystością w sektorze publicznym, jednym z celów jest określenie czy zmiana sytuacji finansowej osób z sektora publicznego jest zgodna z prawem. Generalnie, każda operacja zbierania i/lub publikowania danych powinna być funkcjonalna; na przykład aby ujawnić, że takie osoby w nielegalny sposób nabyły aktywa, naruszyły środki związane z konfliktem interesów lub popełniły nielegalny lub niegodziwy czyn. Nie jest odpowiednim zbieranie oraz dalsze przetwarzanie danych osobowych, które nie są pomocne w ocenie takich naruszeń i/lub wykryciu potencjalnych niewłaściwych zachowań. Zaleca się aby prawne oraz praktyczne ramy były zaprojektowane w taki sposób, aby skupiały się na osiągnięciu uzasadnionego celu zarządzania konfliktami interesów oraz związaną z tym przejrzystością, tak aby zapobiec jakimkolwiek niekoniecznemu, nielegalnemu lub nierzetelnemu przetwarzaniu danych osobowych.

PRZYKŁAD Relacje biznesowe nawiązane podczas sprawowania stanowiska publicznego mogą wskazać na nielegalne postępowanie oraz być przedmiotem głębszej analizy przez odpowiednie instytucje. Dlatego informacje mogą być przetwarzane, jeśli to odpowiednie, w celu weryfikacji czy osoba z sektora publicznego osiągnęła nieproporcjonalny zysk finansowy lub inny, pośrednio lub bezpośrednio (poprzez członka rodziny lub partnera).

3.3 PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH OSOBOWYCH (DANE WRAŻLIWE)

Artykuł 8 ustęp 1 Dyrektywy 95/46/WE stanowi, że dane wrażliwe to dane ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również danych dotyczące zdrowia i życia. Ogólne rozporządzenie rozszerza zakres szczególnych kategorii danych osobowych i obejmuje również dane genetyczne, dane biometryczne pozwalające na jednoznaczną identyfikację osoby oraz dane o orientacji seksualnej. Zarówno Dyrektywa 95/46/WE jak i Ogólne rozporządzenie zawierają jako zasadę ogólną zakaz przetwarzania takich danych, określając kilka wyjątków gdy takie dane mogą być przetwarzane.

Ponadto art. 8 ustęp 5 Dyrektywy 95/46/WE stanowi, że przetwarzanie danych dotyczących przestępstw, wyroków skazujących lub środków bezpieczeństwa może być dokonywane

jedynie pod kontrolą władz publicznych, lub też, jeżeli zgodnie z prawem krajowym ustanowiono określone środki zabezpieczające, z zachowaniem odstępstw, które Państwo Członkowskie może udzielić zgodnie z obowiązującymi przepisami prawa krajowego, zapewniając zachowanie odpowiednich zabezpieczeń. Podobne postanowienia zostały zawarte w Ogólnym rozporządzeniu.

Biorąc pod uwagę powyższe przepisy, pro aktywne ujawnianie takich danych powinno odbywać się wyjątkowo, na podstawie konkretnej podstawy prawnej i zawsze mając na uwadze zachowanie odpowiedniej równowagi pomiędzy ochroną prywatności a uzasadnionym interesem publicznym.

PRZYKŁAD: Jeżeli jest to konieczne w procesie rekrutacyjnym, dopuszczalnym może być publikowanie informacji dotyczących osób wybieranych w wyborach reprezentujących partie polityczne, które ujawniały by ich związki z niektórymi grupami politycznymi lub związkami zawodowymi.

3.4 OKRESY PRZECHOWYWANIA

Okres przechowywania danych osobowych w formie pozwalającej na identyfikację osób, których dane dotyczą powinien być określony zgodnie z uzasadnionym celem, dla którego są one przechowywane. Dane powinny być przetwarzane przez okres konieczny do osiągnięcia tych uzasadnionych celów. Przetwarzanie w ramach właściwych instytucji powinno być rozważane oddzielnie od przetwarzania w celu publikowania danych. Preferowanym jest, aby okresy przechowywania były jasno określone oraz zawierały przepisy dotyczące dostępności danych w Internecie.

Można określić różne okresy: okres przetwarzania danych dla osiągnięcia głównego celu, okres dla celów publikacji tych danych oraz okres archiwizacji. Różne okresy mogą mieć zastosowanie do różnych danych oraz zbiorów.

3.5 JAKOŚĆ DANYCH

Dane osobowe powinny być dokładne oraz, gdzie to konieczne, aktualizowane. Zgodnie z art. 6 Dyrektywy 95/46/WE należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane. Ponadto, zgodnie z Ogólnym rozporządzeniem, osoby z sektora publicznego będą miały prawo uzyskać od odpowiednich instytucji, bez zbędnej zwłoki, poprawienie swoich danych osobowych, które są niedokładne lub nieaktualne. Art. 16 Ogólnego rozporządzenia stanowi także, że z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Jeżeli prawo wymaga aby pewne dane były publikowane w Internecie, zaleca się, w świetle zasady dokładności, aby właściwe instytucje utworzyły jasny/dedykowany formularz, który zawierałoby tylko odpowiednie dane.

Zaleca się również, aby właściwe instytucje wdrożyły odpowiednie procedury aby zachować dokładność oraz aktualność zebranych danych osobowych zgodnie z art. 6 Dyrektywy 95/46/WE oraz Ogólnym rozporządzeniem. Dobrą praktyką jest wskazywanie daty opublikowania, lub przynajmniej aktualizacji, wszelkich opublikowanych zbiorów.

3.6 OGRANICZENIE CELU

Zebrane dane mogą być przetwarzane jedynie w ramach określonych celów oraz dla innych zgodnych celów. Art. 6 ustęp 1 lit. b) Dyrektywy 95/46/WE stanowi, aby dane osobowe były gromadzone do określonych, jednoznacznych i legalnych celów oraz nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem.

Również w Ogólnym rozporządzeniu zawarto podobne przepisy, zgodnie z którymi dane muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami.

Należy zauważyć, że w niektórych państwach członkowskich niektórzy administratorzy danych dodali konkretne informacje, aby określić granice ponownego wykorzystania opublikowanych danych. Jak podkreśliła GR29 w swojej opinii 06/2013 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego, potencjalni ponowni użytkownicy muszą zapewnić zgodność z prawem ochrony danych, tak jak administratorzy danych, kiedy mają do czynienia z danymi osobowymi, chyba że ich operacje przetwarzania wchodziły w zakres wyłączenia dla celów domowych zgodnie z Art. 3 Dyrektywy 95/46/WE.

Przy ocenie czy dane powinny być globalnie dostępne za pomocą zewnętrznych wyszukiwarek, odpowiednim jest mieć na uwadze cel szerokiego udostępnienia danych. Jeżeli istnieje globalny interes publiczny udostępnienia danych, szczególnie mając na uwadze kategorie osób, których dane dotyczą, wtedy takie rozpowszechnienie będzie prawdopodobnie uzasadnione. Stanie się tak pod warunkiem, że jakiegokolwiek potencjalny wpływ na prawa oraz wolności osób, których dane dotyczą został wzięty pod uwagę. Jednakże jeżeli nie istnieje taki globalny interes publiczny lub jeżeli takie szerokie udostępnienie danych zostanie uznane za nieproporcjonalne, zaleca się udostępnienie danych za pomocą wewnętrznych wyszukiwarek internetowych²⁰ lub przez inne selektywne mechanizmy (np. po zalogowaniu się lub przy użyciu technologii captcha).

²⁰ W tym celu, szczególnie zasady dostępu mogą być zakodowane w każdym pliku tekstowym (na przykład poprzez metatagi noindex/noarchive oraz pliki robots.txt, skonfigurowane zgodnie z Robots Exclusion Protocol). Pozostaje to bez uszczerbku dla wykorzystania jakiegokolwiek narzędzi, które mogą ułatwić odzyskanie informacji oraz dokumentów, które mają być rozpowszechnione na stronie internetowej instytucji publicznej.

Zaleca się aby było jasno określone czy ponowne wykorzystanie danych jest dozwolone czy zabronione, a także powinny być określone ewentualne warunki ponownego wykorzystania²¹.

5. ŚRODKI OCHRONNE

Właściwe instytucje, jak administratorzy danych, muszą przyjąć odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym zniszczeniem, utratą, zmianą, nieupoważnionym ujawnieniem lub dostępem oraz wszelkimi innymi niezgodnymi z prawem formami przetwarzania.

W tym celu, należy zastosować odpowiednie środki w celu redukcji ryzyka, że informacje oraz dokumenty dostępne przez Internet mogą być usunięte, poprawione, zmienione oraz/lub wyjęte z kontekstu – na przykład, istnieje możliwość określenia zaufanych źródeł, z których dokumenty te mogą być uzyskane; można wykorzystać podpisy elektroniczne w celu zapewnienia autentyczności oraz integralności dokumentów; można również wprowadzić dane określające kontekst do plików publikowanych na oficjalnych stronach, takie jak określenie wersji dokumentu, termin wygaśnięcia oraz właściwą instytucję administracji odpowiedzialną za informację.

6. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

Aby zapewnić rzetelne przetwarzanie, GR29 zaleca aby odpowiednie instytucje informowały osoby ponownie wykorzystujące informacje o ich obowiązkach związanych z prawami osób, których dane dotyczą oraz odnośnie tego jak zapewnić zgodność z przepisami.

Przed zebraniem jakichkolwiek danych osobowych, właściwe instytucje muszą poinformować osoby z sektora publicznego, których dane są zbierane, zgodnie z art. 10 oraz 11 Dyrektywy 95/46/WE. Prawo do informacji może wynikać z odpowiednich przepisów określających, które dane osobowe powinny być upublicznione i które mogą być z tego powodu opublikowane bez zgody osób z sektora publicznego.

Ponadto osoba, której dane dotyczą musi być w stanie uzyskać następujące informacje od właściwych instytucji, chyba że zastosowanie mają wyjątki określone w dyrektywie 95/46/WE:

- potwierdzenia, czy dotyczące jej dane są przetwarzane oraz co najmniej informacji o celach przetwarzania danych, kategoriach danych oraz odbiorcach lub kategoriach odbiorców, którym dane te są ujawniane,

²¹ Zobacz Opinia GR29 WP207

- wyrażonej w zrozumiałej formie informacji o danych przechodzących przetwarzanie oraz posiadanych informacji o ich źródłach,
- wiadomości na temat zasad automatycznego przetwarzania dotyczących jej danych przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego.

Zgodnie z art. 14 Dyrektywy 95/46/WE, w niektórych przypadkach²² osoba, której dane dotyczą ma prawo złożenia sprzeciwu dotyczącego przetwarzania w dowolnym czasie. Zaleca się, aby administrator informował wszystkie podmioty ponownie wykorzystujące takie dane o sprzeciwie.²³

Prawo do sprzeciwu może nie mieć zastosowania lub być ograniczone w zależności od celu. Na przykład może ono pozwalać osobom, których dane dotyczą złożyć sprzeciw wobec publikacji w Internecie niektórych lub wszystkich danych ich dotyczących w oparciu o przeważające uzasadnione interesy odnoszące się do ich szczególnej sytuacji ale nie wobec wewnętrznych operacji przetwarzania (sytuacja inna niż rozpowszechnianie dotyczących ich danych).

Również każda osoba, której dane dotyczą musi być w stanie uzyskać od odpowiednich instytucji poprawienie, usunięcie lub zablokowanie danych, których przetwarzanie jest niezgodne z Dyrektywą 95/46/WE. Co więcej, strony trzecie, którym ujawniono dane muszą być poinformowane o takim poprawieniu, usunięciu lub zablokowaniu, chyba że okazałoby się to niemożliwe lub pociągało by za sobą nieproporcjonalne środki.

Zgodnie z Ogólnym rozporządzeniem osoba, której dane dotyczą będzie miała prawo do poprawienia, usunięcia lub ograniczenia przetwarzania danych, jak również prawo do złożenia skargi do organu ochrony danych.

²² W tym kontekście należy wspomnieć, że art. 14 Dyrektywy stanowi, że osoba, której dane dotyczą może skorzystać z prawa do wyrażenia sprzeciwu przynajmniej, między innymi, w przypadkach wymienionych w art. 7 lit. e) Dyrektywy. Oznacza to, że jeżeli przetwarzanie jest dopuszczone, poza rozsądną oraz obiektywną oceną różnych pra oraz interesów w danej sprawie, osoba, której dane dotyczą ciągle ma możliwość wyrażenia sprzeciwu na podstawie dotyczącej jej sytuacji. Zobacz przywołaną już Opinię GR29 06/4014, Część III, ustęp 3.6.

²³ We Francji obowiązek taki jest ustanowiony w art. 97 dekretu dotyczącego krajowej ustawy o ochronie danych.