PANOPTYKON
FUNDACJA

Zarząd: Katarzyna Szymielewicz, Małgorzata Szumańska
Rada programowa: Adam Bodnar, Ewa Charkiewicz, Dominika Dörre-Nowak, Józef Halbersztadt, Joanna Kamiol, Monika Płatek, Maciej Ślusarek, Piotr Waglowski, Roman Wieruszewski

Warszawa, 6 kwietnia 2012 r.

Uwagi Fundacji PANOPTYKON do projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych

W odpowiedzi na zaproszenie Ministerstwa Spraw Wewnętrznych do zgłaszania uwag do projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych (dalej: **projekt dyrektywy**) przedstawiamy nasze wstępne stanowisko. Niniejszy dokument stanowi rozwinięcie i uzupełnienie kierunkowych uwag do projekty dyrektywy, które przekazaliśmy Państwu drogą mailową 21 marca 2012 roku.

Zastrzegamy jednocześnie, że – ze względu na relatywnie krótki czas konsultacji – nasza analiza nie jest wyczerpująca. Mamy nadzieję, że okazja do zgłoszenia pogłębionych uwag pojawi się jeszcze na dalszych etapach pracy nad tym projektem.

1. Zakres zastosowania

Bardzo poważne wątpliwości wzbudza ograniczony zakres zastosowania zasad ochrony danych osobowych wyrażonych w projekcie dyrektywy. Zgodnie z art. 2, dyrektywa nie ma mieć zastosowania do przetwarzania danych osobowych w ramach działalności wykraczającej poza zakres prawa Unii, w szczególności dotyczącej bezpieczeństwa narodowego.

Wydaje się, że to wyłączenie stwarza bardzo szeroką możliwość omijania zasad ochrony danych osobowych przez organy egzekwowania prawa. Wyznaczenie granicy między walką ze "zwykłą" przestępczością a zapobieganiem zagrożeniom istotnym z perspektywy bezpieczeństwa narodowego może być w konkretnych przypadkach bardzo trudne. Zachowanie tego generalnego wyłączenia może też utrudnić organom ochrony danych realizację ich uprawnień nadzorczych, a obywatelom – realizację ich praw podmiotowych. Naszym zdaniem konieczne jest sprecyzowanie, jakich dokładnie sytuacji dotyczy to i inne – omawiane niżej – wyłączenia, które pojawiają się w projekcie dyrektywy.

2. Zasady dotyczące przetwarzania danych osobowych

Zwracamy uwagę na bardzo ogólne sformułowanie zasad ochrony danych w projekcie dyrektywy, który wciąż pozostawia bardzo duży margines interpretacji poszczególnym państwom członkowskim. Sformułowania zaproponowane w art. 4 nie rozstrzygają podstawowych dylematów, z jakimi muszą się mierzyć przedstawiciele organów egzekwowania prawa w swoich działaniach. W szczególności projekt nie rozstrzyga, czy dopuszczalne jest rutynowe pobieranie i przetwarzanie danych osobowych wszystkich obywateli lub danej kategorii obywateli w celach prewencyjnych (np. w ramach systemów takich jak PNR lub SWIFT).

Projekt nie odnosi się do niektórych z katalogu podstawowych zasad ochrony danych, takich jak przejrzystość i prawidłowość danych. Artykuł 4 w obecnym kształcie nie zawiera również propozycji jasnego uregulowania zasad wykorzystywania na potrzeby bezpieczeństwa publicznego danych zbieranych (pierwotnie) w celach komercyjnych (np. w ramach istniejących systemów PNR czy reżimu obowiązkowej retencji danych telekomunikacyjnych). Autorzy projektu podjęli próbę uregulowania tej materii w pierwszym projekcie dyrektywy (art. 4 ust. 2), jednak te przepisy zostały wykreślone z wersji aktualnie poddawanej konsultacjom.

Zwracamy również uwagę na problem ograniczenia zakresu stosowania zasad ochrony danych osobowych ze względu na poddanie danych procesowi anonimizacji. Zgodnie z aktualną treścią art. 4, dane powinny być „przechowywane w formie umożliwiającej identyfikację podmiotów danych przez czas nie dłuższy niż jest to konieczne do celów, dla których dane są przetwarzane". Tym samym, ograniczenie czasu przechowywania danych nie ma mieć zastosowania do danych, które zostały poddane anonimizacji.

Założenie, że dane osobowe można w sposób skuteczny i nieodwracalny poddać anonimizacji budzi poważne wątpliwości wśród inżynierów rozwijających praktyczne technologie ochrony danych. Przy dzisiejszym rozwoju technologicznym, trudno jest jednoznacznie ocenić, czy dokonano skutecznej anonimizacji. Proces taki powinien doprowadzić do tego, że przetwarzane przez administratora informacje nie będą pozwalać na identyfikację osoby. W naszej ocenie „przechowywane w formie umożliwiającej identyfikację podmiotów danych" nie powinno w sposób automatyczny wyłączać danych spod reżimu ochronnego, szczególnie dopóki warunki, jakie powinna spełniać skuteczna anonimizacja nie zostaną jasno sprecyzowane.

3. Przetwarzanie szczególnych kategorii danych osobowych

Nasze wątpliwości wzbudza szeroki zakres wyłączeń przewidziany w art. 8, dotyczącym przetwarzania szczególnych kategorii danych osobowych. Co do zasady projekt dyrektywy zabrania przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, wierzenia religijne lub przekonania filozoficzne, przynależność do związków zawodowych, oraz przetwarzania danych genetycznych lub danych dotyczących zdrowia i życia seksualnego.

To ograniczenie nie ma mieć jednak zastosowania, gdy na przetwarzanie szczególnych kategorii danych osobowych zezwala „prawo przewidujące odpowiednie gwarancje" lub jest ono niezbędne „w celu ochrony żywotnych interesów podmiotu danych lub innej osoby" lub przetwarzanie dotyczy danych, które „zostały wyraźnie podane do publicznej wiadomości" przez ich podmiot.

W naszej opinii są to bardzo szerokie wyłączenia, otwarte na różne interpretacje i praktyki stosowania. Konieczne jest zatem bardziej szczegółowe zdefiniowanie, jakich przypadków dotyczą wspomniane wyjątki od ogólnego zakazu przetwarzania szczególnych kategorii danych. W obecnym kształcie dyrektywy, wyłączenia te mają zbyt ogólny charakter i mogą prowadzić do poważnych problemów interpretacyjnych.

4. Środki oparte na profilowaniu i automatycznym przetwarzaniu

Bardzo pozytywnie oceniamy próbę uregulowania praktyk profilowania i przyjęcie zasady, że osoba może być poddana profilowaniu tylko w ściśle określonych, przewidzianych prawem sytuacjach. Treść art. 9, który reguluje tę problematykę, może budzić jednak poważne wątpliwości interpretacyjne.

Nie jest dla nas jasne, jak może być interpretowane podstawowe kryterium uznania danej czynności za profilowanie, a mianowicie wymóg „wywoływania niekorzystnych skutków prawnych dla podmiotu danych, lub wywierania istotnego wpływu na daną osobę". W naszej opinii jest to kryterium zbyt wąskie i może prowadzić do sytuacji, gdy przyjęty jako zasada zakaz stosowania środków opartych na profilowaniu i automatycznym przetwarzaniu będzie ograniczany w sposób nieuzasadniony.

Nasze wątpliwości budzi również zakres wyłączeń od ogólnego zakazu profilowania, a mianowicie przyjęcie, że zakaz ten nie stosuje się, jeśli profilowanie „zostanie dopuszczone prawem, które przewiduje również gwarancje słusznych interesów podmiotu danych". W naszej opinii jest to sformułowanie zbyt ogólne i nie gwarantuje odpowiedniego poziomu ochrony praw podmiotu danych. Profilowanie powinno być dopuszczalne jedynie w oparciu o ścisły test niezbędności i proporcjonalności, czyli wykazanie, że jest ono w danej sytuacji konieczne i nie narusza żywotnych interesów osoby, której dotyczy.

5. Zakres obowiązku informacyjnego i ograniczenia prawa do dostępu do informacji o przetwarzaniu danych

Bardzo pozytywnie przyjęliśmy próbę zagwarantowania praw podmiotów danych wobec organów wymiaru sprawiedliwości i egzekwowania prawa, w tym prawa do dostępu do informacji na temat przetwarzanych danych. Nasze wątpliwości budzi jednak przewidziany zakres wyłączeń oraz nieprecyzyjne określenie zasad, które wyznaczają zakres prawa podmiotu danych oraz skorelowanego z nim obowiązku administratora danych.

W szczególności art. 11 dopuszcza odstępstwa od obowiązku informowania, o ile stanowią one "konieczny i proporcjonalny środek w demokratycznym społeczeństwie, przy należytym uwzględnieniu słusznych interesów danej osoby". Jak pokazuje chociażby europejska debata na temat obowiązkowej retencji danych, test „konieczności i proporcjonalności" jest podatny na różne interpretacje w zależności od kultury prawnej i aktualnego kontekstu politycznego. Na podstawie tak ogólnej zasady nie sposób zagwarantować podobnych standardów ochrony praw podmiotów danych w Unii Europejskiej.

Opóźnienie, ograniczenie lub wyłączenie informowania jest możliwe m.in. w celu ochrony bezpieczeństwa publicznego lub bezpieczeństwa narodowego – wątpliwości w tym przypadku wzbudza zarówno trudność z rozgraniczeniem tych kategorii, jak również możliwość szerokiego ich interpretowania. Także pojęcia "utrudnianie" (lit. a) i "negatywny wpływ" (lit. b) nie są

wystarczająco ostre, co stwarzają dodatkowe pole do nadużyć.

Analogiczne wątpliwości wzbudza treść art. 13, który przewiduje możliwość ograniczenia (w całości lub części) prawa dostępu podmiotu do danych, o ile stanowi ono „konieczny i proporcjonalny środek w demokratycznym społeczeństwie, przy należytym uwzględnieniu słusznych interesów danej osoby". Podobnie jak w przypadku art. 11, mamy zastrzeżenia dotyczące sformułowań zawartych w ust. 1 lit. a-d.

W zakresie dostępu do przetwarzanych danych warto w naszej opinii rozważyć rozszerzenie zakresu informacji udzielanych podmiotowi danych o informacje, które mają być zbierane na podstawie art. 24 projektu dyrektywy (ewidencja), w szczególności o cel, w jakim konkretne osoby uzyskiwały wgląd do danych. Pozwoli to podmiotowi danych na pełniejszą ocenę, czy dotyczące go informacje są przetwarzane zgodnie z prawem.

6. Przetwarzania danych przez współadministratorów

Zgodnie z art. 20, w przypadku gdy administrator określa cele, warunki i środki przetwarzania danych osobowych wspólnie z innymi administratorami „współadministratorzy muszą ustalić zakres odpowiedzialności za zgodność z obowiązkami wynikającymi z niniejszej dyrektywy spoczywającej na każdym z nich, w szczególności w odniesieniu do procedur i mechanizmów wykonywania praw podmiotu danych w drodze wspólnych uzgodnień".

Obawiamy się, że *w*prowadzenie takiego rozwiązania może w praktyce prowadzić do obniżenia standardu ochrony danych osobowych przewidzianego w dyrektywie w drodze umowy między współadministratorami. W naszej opinii każdy administrator powinien być zobowiązany do zachowania pewnych minimalnych standardów.

7. Zasady ochrony danych w przypadku transferu do państw trzecich

Rozdział V określa ogólne zasady przekazywania danych do państw trzecich lub organizacji międzynarodowych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, w tym wtórnego przekazywania. Zgodnie z podstawową zasadą wyrażoną w art. 33, przekazywanie do państw trzecich może mieć miejsce jedynie wtedy, gdy jest to „niezbędne do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania i w celu wykonywania kar kryminalnych" oraz gdy administrator i podmiot przetwarzający spełniają określone warunki, w szczególności gdy zapewniony jest odpowiedni poziom ochrony danych osobowych.

Jednocześnie, kolejne artykuły rozdziału V, w szczególności art. 35 ust. 1 pkt b oraz art. 36 wprowadzają bardzo szerokie odstępstwa od tej ogólnej zasady, które mogą doprowadzić do systemowych nadużyć i faktycznego omijania – wciąż bardzo ogólnych – podstawowych zasad ochrony danych w sytuacji transferu do państw trzecich wyrażonych w art. 33.

8. Uprawnienia Komisji Europejskiej do wydawania aktów delegowanych i wykonawczych

Artykuł 56 projektu dyrektywy potwierdza uprawnienie Komisji Europejskiej do wydawania aktów o charakterze nieustawodawczym o powszechnym zakresie stosowania, które uzupełniają lub zmieniają niektóre, inne niż zasadnicze, elementy aktu ustawodawczego. Wydaje się, że te kompetencje Komisji powinny zostać szczegółowo zrewidowane i ograniczone do

sytuacji, w których jednostronna decyzja tego organu nie będzie w stanie wpłynąć negatywnie na poziom ochrony danych osobowych zagwarantowany w projekcie dyrektywy. W wielu przypadkach są to kwestie zbyt ważne i zbyt ściśle związane ze sferą praw i wolności obywatelskich, aby mogły być pozostawione w gestii samej Komisji Europejskiej. Doświadczenie pokazuje, że formalna „procedura sprawdzająca" realizowana przez Parlament Europejski, nie jest w stanie zniwelować tych zagrożeń.

W imieniu Fundacji PANOPTYKON

Katarzyna Szymielewicz
Prezes Zarządu

Małgorzata Szumańska
Członkini Zarządu