RADA UNII EUROPEJSKIEJ

Bruksela, 27 stycznia 2012 r. (14.02) (OR. en)

5833/12 ADD 2

Międzyinstytucjonalny numer referencyjny: 2012/0010 (COD)

DATAPROTECT 6
JAI 41
DAPIX 9
FREMP 8
COMIX 59
CODEC 217

PISMO PRZEWODNIE

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Data otrzymania:	27 stycznia 2012 r.
Do:	Uwe CORSEPIUS, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	SEC(2012) 73 final
Dotyczy:	Dokument roboczy służb Komisji Streszczenie oceny skutków towarzyszące rozporządzeniu 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) i dyrektywie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych

Delegacje otrzymują w załączeniu dokument Komisji SEC(2012) 73 final.

Zał.: SEC(2012) 73 final

KOMISJA EUROPEJSKA

Bruksela, dnia 25.1.2012 r.
SEK(2012) 73 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE OCENY SKUTKÓW

towarzyszące dokumentom:

rozporządzenie 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)
i
dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych

{COM(2012) 11 final}
{SEC(2012) 72 final}

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE OCENY SKUTKÓW

towarzyszące dokumentom:

rozporządzenie 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)
i
dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych

1. WPROWADZENIE

Od momentu wprowadzenia w 1995 r. obecnych ram prawnych UE w zakresie ochrony danych szybki rozwój technologiczny i gospodarczy przyniósł nowe wyzwania w zakresie ochrony danych. Niezwykle wzrosła skala wymiany i zbierania danych. Technologia umożliwia zarówno przedsiębiorcom prywatnym, jak i organom publicznym wykorzystywanie danych osobowych do wykonywania powierzonych im zadań na niespotykaną dotąd skalę. Osoby fizycznie coraz częściej udostępniają informacje osobowe publicznie i globalnie, nie zdając sobie w pełni sprawy, jakie z tym wiążą się ryzyka.

Budowanie zaufania do internetu jest kluczowym elementem rozwoju gospodarczego. Brak zaufania sprawia, że konsumenci nie są pewni, czy kupować w internecie i korzystać z nowych usług, w tym elektronicznych usług administracji państwowej (ang. *e-government*). Jeśli nie uda się znaleźć odpowiedniego rozwiązania, ten brak zaufania będzie nadal spowalniać rozwój innowacyjnego wykorzystania nowych technologii, stanowić przeszkodę we wzroście gospodarczym i uniemożliwiać sektorowi publicznemu czerpanie potencjalnych korzyści z cyfryzacji jego usług.

Ponadto traktat lizboński stworzył w art. 16 TFUE nową podstawę prawną bardziej nowoczesnego i kompleksowego podejścia do ochrony danych i swobodnego przepływu danych osobowych, obejmującego również współpracę policyjną i współpracę wymiarów sprawiedliwości w sprawach karnych.

2. OPIS PROBLEMU

Ocena skutków przedstawia i analizuje trzy główne obszary problematyczne:

2.1. Problem nr 1: bariery dla przedsiębiorców i organów publicznych wynikające z rozdrobnienia, niepewności prawnej i niespójnego egzekwowania

Pomimo celu dyrektywy, jakim jest zapewnienie równorzędnego poziomu ochrony danych w UE, w przepisach obowiązujących w państwach członkowskich nadal istnieją istotne rozbieżności. W związku z tym administratorzy danych mogą być zmuszeni do radzenia sobie z 27 różnymi krajowymi systemami i wymogami prawnymi w UE. Wynikiem tego jest rozdrobnione otoczenie prawne, w którym występuje brak pewności prawnej i nierówna ochrona osób fizycznych. Taka sytuacja doprowadziła do niepotrzebnych kosztów i **obciążeń administracyjnych** (w wysokości **około 3 mld EUR rocznie** w scenariuszu bazowym) dla przedsiębiorców i stanowi czynnik zniechęcający tych przedsiębiorców, w tym MŚP, działających na jednolitym rynku, którzy mogą planować rozszerzenie swojej działalności na rynki zagraniczne.

Ponadto zasoby i uprawnienia organów krajowych odpowiedzialnych za ochronę danych znacznie różnią się między państwami członkowskimi. W niektórych przypadkach oznacza to, że nie są one w stanie w satysfakcjonujący sposób wykonywać swoich zadań w zakresie egzekwowania przepisów. Współpraca między tymi organami na szczeblu europejskim – za pośrednictwem istniejącej grupy doradczej (Grupa Robocza Art. 29) – nie zawsze prowadzi do spójnego egzekwowania, zatem także wymaga ulepszenia.

2.2. Problem nr 2: trudności dla osób fizycznych związane z kontrolowaniem przez nie danych osobowych, które ich dotyczą

Biorąc pod uwagę brak harmonizacji krajowych przepisów dotyczących ochrony danych i różne uprawnienia krajowych organów ds. ochrony danych, osobom fizycznym w niektórych państwach członkowskich jest trudniej egzekwować swoje prawa niż w innych, zwłaszcza w kontekście usług internetowych.

Osoby fizyczne straciły także kontrolę nad własnym danymi w związku z tym, że codziennie wymianie podlega bardzo duża ilość danych oraz ze względu na fakt, że osoby te nie są w pełni świadome, iż ich dane są zbierane. Chociaż wielu Europejczyków uważa, że ujawnianie danych osobowych jest w coraz większym stopniu częścią współczesnego życia[1], 72 % użytkowników internetu w Europie nadal uważa, że w środowisku *online* musi podawać zbyt wiele danych osobowych, często nie wiedząc, jak egzekwować swoje prawa *online*.

2.3. Problem nr 3: luki i nieścisłości w ochronie danych osobowych w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych

Zakres dyrektywy, oparty na podstawie prawnej dotyczącej rynku wewnętrznego, wyraźnie wyklucza współpracę policyjną i współpracę wymiarów sprawiedliwości w sprawach karnych. Decyzja ramowa przyjęta w 2008 r. w celu regulacji przetwarzania danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych odzwierciedla specyfikę przedlizbońskiej „struktury filarów" UE i charakteryzuje się **ograniczonym zakresem i różnymi innymi lukami**, często wywołując poczucie niepewności prawnej u osób fizycznych i organów egzekwowania prawa, a także prowadząc do praktycznych trudności we wdrażaniu. Ponadto decyzja ramowa przewiduje szereg

---

[1] Zob. specjalna ankieta Eurobarometru nr 359 – „Stosunek do ochrony danych i tożsamości elektronicznej w Unii Europejskiej", czerwiec 2011 r., s. 23.

możliwości odstąpienia od ogólnych zasad ochrony danych na szczeblu krajowym, zatem nie prowadzi do ich ujednolicenia. Może to doprowadzić do pozbawienia tych zasad możliwości realizacji leżącego u ich podstaw celu, a przez co niekorzystnie wpłynąć na podstawowe prawo osób fizycznych do ochrony ich danych osobowych w tym obszarze, lecz także utrudnia sprawną wymianę danych osobowych między odpowiednimi organami krajowymi.

3. ANALIZA ZASADY POMOCNICZOŚCI I PROPORCJONALNOŚCI

W świetle problemów zarysowanych powyżej analiza zasady pomocniczości wskazuje na potrzebę działania na szczeblu UE na podstawie następujących przesłanek:

- prawo do ochrony danych osobowych jest zapisane w art. 8 Karty praw podstawowych. Artykuł 16 TFUE jest podstawą prawną przyjęcia przepisów UE dotyczących ochrony danych;
- dane osobowe mogą być przekazywane ponad granicami krajowymi, zarówno wewnętrznymi granicami UE, jak i do państw trzecich, w coraz szybszym tempie; ponadto istnieją praktyczne wyzwania w zakresie egzekwowania przepisów dotyczących ochrony danych, zachodzi również potrzeba współpracy między państwami członkowskimi i ich organami, którą należy zorganizować na szczeblu UE, by zagwarantować konieczną spójność i wysoki poziom ochrony w Unii;
- państwa członkowskie nie mogą same ograniczyć problemów w obecnej sytuacji. Dotyczy to zwłaszcza problemów wynikających z rozdrobnienia w krajowych przepisach wdrażających ramy regulacyjne UE w zakresie ochrony danych;
- państwa członkowskie mogłyby przyjąć polityki, dzięki którym prawo to nie byłoby naruszane, jednak w braku wspólnych przepisów unijnych nie byłoby możliwe osiągnięcie jednolitości w tym zakresie i wiązałoby się z ryzykiem wystąpienia ograniczeń w transgranicznych przepływach danych osobowych.

Przewidywane działania są proporcjonalne, gdyż objęte są zakresem kompetencji Unii zdefiniowanych w Traktatach i są niezbędne, by zapewnić jednolitość stosowania prawodawstwa UE zapewniającego skuteczną i równą ochronę podstawowych praw osób fizycznych. Działanie na szczeblu UE jest niezbędne, by nadal gwarantować wiarygodność i wysoki poziom ochrony danych w zglobalizowanym świecie, utrzymując jednocześnie swobodny przepływ danych. Odpowiednie funkcjonowanie rynku wewnętrznego wymaga, by przepisy zapewniały podmiotom gospodarczym równe szanse.

4. CELE

Trzy główne **cele polityki** są następujące:

- **zwiększyć wymiar ochrony danych** związany z rynkiem wewnętrznym poprzez zmniejszenie rozdrobnienia, poprawę spójności i **uproszczenie** środowiska regulacyjnego, eliminując tym samym niepotrzebne koszty i **zmniejszając obciążenie administracyjne**;

- **podwyższyć skuteczność podstawowego prawa do ochrony danych i umożliwić osobom fizycznym kontrolę dotyczących ich danych**;

- **zwiększyć spójność unijnych ram ochrony danych**, w tym w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, z pełnym uwzględnieniem wejścia w życie traktatu lizbońskiego.

5. WARIANTY POLITYKI

5.1. Wariant nr 1: działanie „miękkie"

Wariant ten opiera się w głównej mierze na **komunikatach Komisji zawierających wykładnię, narzędziach wsparcia technicznego oraz finansowaniu**, a także **zachęcaniu do standaryzacji i samoregulacji**, by wzmocnić praktyczne wdrażanie obowiązujących przepisów przez administratorów danych i podnieść świadomość osób fizycznych. Komisja zaproponowałaby **wyłącznie bardzo ograniczone zmiany legislacyjne** służące wyjaśnieniu pojęć zawartych w dyrektywie i dotyczące konkretnych kwestii, których nie można rozstrzygnąć w inny sposób. Ten wariant polityki byłby odpowiedni jedynie dla problemów nr 1 i 2.

Ograniczone zmiany legislacyjne wyraźnie wprowadziłyby zasadę przejrzystości i minimalizacji danych, a także podstawę prawną „wiążących reguł korporacyjnych" dla międzynarodowych operacji przekazywania.

5.2. Wariant nr 2: bardziej nowoczesne ramy prawne

Komisja przedstawiłaby **wnioski ustawodawcze mające na celu jeszcze większą harmonizację przepisów materialnych**, wyjaśnienie przepisów szczególnych oraz usunięcie niespójności spowodowane różnym podejściem państw członkowskich. Wnioski te dotyczyłyby problemu nr 1 i 2, gdyż z jednej strony **ułatwiałyby przepływy danych w ramach UE oraz z UE do państw trzecich**, zaś z drugiej strony **wyjaśniałyby i wzmacniały prawa osób fizycznych** (np. prawo dostępu, „prawo do bycia zapomnianym", bardziej zrozumiałe sposoby wyrażania zgodny oraz zgłaszania naruszenia ochrony danych), a także **zwiększały odpowiedzialność oraz „rozliczalność" administratorów danych i podmiotów przetwarzających** dane (np. poprzez wprowadzenie, w stosownych przypadkach, obowiązku wyznaczenia inspektorów ochrony danych lub przeprowadzenia oceny skutków w zakresie ochrony danych). Wariant ten ustanawiałby w szczególności **„punkt kompleksowej obsługi"** dla administratorów danych (tj. jedne przepisy i jeden odpowiedzialny organ ds. ochrony danych). Ogólne wymogi w zakresie zgłaszania zostałyby uproszczone (tj. „podstawowa rejestracja"). **Zwiększałby także niezależność organów ds. ochrony danych i harmonizował ich uprawnienia**. Współpraca i wzajemna pomoc organów ds. ochrony danych zostałyby zacieśnione, w tym dzięki nowemu **„mechanizmowi zgodności"** obejmującemu zarówno nowo ustanowioną „Europejską Radę Ochrony Danych", jak i Komisję.

Jeśli chodzi o ochronę danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych (problem nr 3), Komisja przedstawiłaby wnioski, które zastąpiłyby decyzję ramową **nowym instrumentem o rozszerzonym zakresie** oraz wypełniłyby **najważniejsze luki i braki**, by wzmocnić prawa osób fizycznych i ułatwić współpracę między organami ścigania, przy jednoczesnym uwzględnieniu specyfiki sektora egzekwowania prawa.

5.3. Wariant nr 3: szczegółowe przepisy prawne na szczeblu UE

Wariant ten obejmowałby większość elementów wariantu nr 2, a także o **wiele bardziej szczegółowe przepisy UE**, w tym przepisy sektorowe (np. w sektorze opieki zdrowotnej i medycznym) oraz **scentralizowaną strukturę egzekwowania prawa na szczeblu UE** (tj. ustanowienie Organu Ochrony Danych UE). Polegałby także na wyeliminowaniu ogólnych wymogów w zakresie zgłaszania (z wyjątkiem uprzedniego sprawdzenia ryzykownego przetwarzania), ustanowieniu ogólnounijnego systemu certyfikacji procesów i produktów w zakresie rozpatrywania skarg związanych z ochroną danych oraz zdefiniowaniu zharmonizowanych w całej UE kar kryminalnych za naruszenie przepisów o ochronie danych. Zgoda zostałaby zdefiniowana jako „główna podstawa" przetwarzania danych.

Jeśli chodzi o współpracę policyjną i współpracę wymiarów sprawiedliwości w sprawach karnych, poza środkami materialnymi o których mowa w wariancie nr 2, wariant ten obejmowałby ustanowienie szczegółowych przepisów w zakresie prawa dostępu (zawsze bezpośredniego) osób fizycznych. Polegałby także na **zmianie właściwych przepisów wszystkich obowiązujących instrumentów z dawnego trzeciego filara**, by dopasować je do nowych, rozszerzonych przepisów zharmonizowanych.

6. OCENA SKUTKÓW

6.1. Wariant polityki nr 1: działanie „miękkie"

Komunikaty Komisji zawierające wykładnię przepisów dyrektywy nie byłyby wiążące, zatem miałyby **jedynie ograniczony wpływ na zmniejszenie niepewności prawnej i kosztów**. Większa samoregulacja na szczeblu UE pomogłaby w zapewnieniu administratorom danych większej jasności prawa w poszczególnych sektorach, **nie byłaby jednak wystarczająca**, by zapewnić skuteczne i spójne stosowanie przepisów w braku jasnych i zharmonizowanych ram prawnych UE leżących u jej podstaw.

Kampanie informacyjne pomogłyby osobom fizycznym w lepszym poznaniu ich praw oraz lepszym zrozumieniu praktycznych sposobów ich egzekwowania. **Nie wystarczyłoby** to jednak do wyraźnego określenia praw osób fizycznych, gdyż przepisy prawa nie definiują tych praw w wyraźny sposób. **Wyjaśnienie przepisów** dotyczących zasad przejrzystości, minimalizacji danych, odpowiedniości i wiążących reguł korporacyjnych zwiększyłoby harmonizację i pewność prawną dla osób fizycznych i przedsiębiorców.

Jeśli chodzi o egzekwowanie, komunikaty Komisji nie przezwyciężyłyby niechęci państw członkowskich do zmiany krajowych przepisów w taki sposób, by dać organom ds. ochrony danych większą niezależność i zharmonizowane uprawnienia. Większa koordynacja przez Grupę Roboczą Art. 29 i wymiany między organami ds. ochrony danych miałyby pozytywny wpływ na spójniejsze egzekwowanie przepisów, jednak **nadal istniejące rozbieżności w krajowych przepisach i ich interpretacji ograniczałyby efekt pogłębionej współpracy miedzy organami ds. ochrony danych**.

Spodziewane **skutki finansowe i gospodarcze tego wariantu polityki są ograniczone** i zidentyfikowane problemy w dużej mierze pozostałyby nierozwiązane.

6.2. Wariant polityki nr 2: bardziej nowoczesne ramy prawne

Niepewność prawna dla przedsiębiorstw prywatnych i organów publicznych **zostanie znacznie zmniejszona**. Problematyczne przepisy zostaną wyjaśnione i wzrośnie spójność w związku z mniejszym marginesem interpretacji oraz przyjmowaniem środków wykonawczych lub aktów delegowanych przez Komisję.

Zastąpienie ogólnego zgłoszenia przetwarzania danych uproszczonym **zharmonizowanym systemem „rejestracji"**, przy jednoczesnym zachowaniu uprzednich kontroli pod kątem wrażliwych danych i przetwarzania danych zwolni administratorów danych z obowiązku, który jest obecnie realizowany w różny sposób. Zwiększenie odpowiedzialności administratorów danych i podmiotów przetwarzających dane poprzez wprowadzenie, w niektórych przypadkach i przy wyraźnie zdefiniowanych i wyznaczonych progach, inspektorów ochrony danych i ocen skutków w zakresie ochrony danych oraz wprowadzenie zasady uwzględnienia ochrony danych już w fazie projektowania będą oznaczać łatwiejsze zapewnienie i wykazanie zgodności.

Wyjaśnienie i uproszczenie przepisów poprzez zdefiniowane jednego systemu prawa mającego zastosowanie w całej Unii oraz ustanowienie „punktu kompleksowej obsługi" na rzecz nadzoru w zakresie ochrony danych wzmocni rynek wewnętrzny, w tym poprzez usunięcie różnic w zakresie formalności administracyjnych, którym muszą sprostać organy ds. ochrony danych. Umożliwi to **zaoszczędzenie w sumie**, tylko jeśli chodzi o obciążenie administracyjne, około **2,3 mld EUR** rocznie.

Zwiększy się także spójność egzekwowania przepisów dzięki wzmocnieniu i harmonizacji uprawnień organów ds. ochrony danych, a także zacieśnieniu współpracy i stworzeniu mechanizmu wzajemnej pomocy w przypadkach o wymiarze unijnym oraz zharmonizowaniu czynów podlegających sankcjom administracyjnym.

Ogólnounijny zharmonizowany obowiązek zgłaszania naruszeń ochrony danych będzie lepiej chronić osoby fizyczne, zapewni spójność w różnych sektorach i pomoże uniknąć niekorzystnych skutków konkurencji.

Poprzez wprowadzenie nowych praw, a także poprawę i lepsze wyjaśnienie istniejących praw **znacznemu wzmocnieniu uległyby prawa podmiotów danych i kontrola osób fizycznych nad swoimi danymi**. Dzieci skorzystają na środkach, które w szczególny sposób uwzględniają ich podatność na zagrożenia. Zrzeszenia będą mogły w większym zakresie wspierać podmioty danych w egzekwowaniu przez nie praw, w tym w postępowaniach przed sądem.

Stosowanie ogólnych zasad ochrony danych do obszarów współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych zwiększyłoby ogólną spójność unijnych ram ochrony danych, przy jednoczesnym poszanowaniu specyfiki egzekwowania przepisów. Prawa osób fizycznych zostałyby wzmocnione w szczególności poprzez rozszerzenie zakresu przepisów dotyczących ochrony danych w tym obszarze na przetwarzanie o charakterze „domowym", ustanowienie warunków zapewnienia prawa dostępu i opracowanie bardziej rygorystycznych przepisów w zakresie ograniczenia celu.

Jeśli chodzi o **wpływ finansowy i gospodarczy**, obowiązek wyznaczania inspektorów ochrony danych przez większe podmioty gospodarcze (zatrudniające ponad 250 pracowników) nie **pociągnie za sobą niewspółmiernie dużych kosztów**, gdyż inspektorzy

ochrony danych niejednokrotnie pracują już w tych przedsiębiorstwach. Koszty zapewnienia zgodności nie przekroczyłyby 320 mln EUR rocznie. Obowiązek ten objąłby niezbędną minimalną liczbę administratorów danych, gdyż MŚP byłyby co do zasady wykluczone z tego obowiązku, chyba że prowadzona przez nie działalność w zakresie przetwarzania wiązałaby się ze znacznym ryzykiem dla przetwarzania danych. Organy i podmioty publiczne mogłyby wyznaczać jednego inspektora ochrony danych dla kilku podmiotów (np. kilku oddziałów, ministerstw, urzędów), uwzględniając własną strukturę organizacyjną.

Uproszczenie przepisów dotyczących międzynarodowego przekazywania (na przykład poprzez rozszerzenie zakresu „wiążących reguł korporacyjnych") także miałoby pozytywny wpływ na konkurencyjność przedsiębiorstw unijnych na arenie międzynarodowej.

Wzmocnienie niezależności i uprawnień organów ds. ochrony danych, wraz z obowiązkiem przekazywania im przez państwa członkowskie wystarczających zasobów, wiązałoby się z dodatkowymi kosztami dla organów publicznych, które nie mają obecnie właściwych uprawnień i odpowiednich zasobów.

Nowy mechanizm współpracy i wzajemnej pomocy między organami ds. ochrony danych także wiązałby się z koniecznością poniesienia przez krajowe organy ds. ochrony danych oraz Europejskiego Inspektora Ochrony Danych (EIOD) dodatkowych kosztów. Na przykład dodatkowe zadania EIOD w zakresie zapewnienia obsługi sekretariatu Europejskiej Rady Ochrony Danych – zastępującej Grupę Roboczą Art. 29 – w szczególności zaangażowanie w mechanizm zgodności będą prawdopodobnie wymagać zwiększenia obecnych zasobów o kolejne 3 mln EUR rocznie średnio przez pierwsze sześć lat, w tym środków na 10 dodatkowych etatów.

6.3. Wariant nr 3: szczegółowe przepisy prawne na szczeblu UE

Dodanie kolejnych szczegółowych przepisów prawnych, w tym sektorowych, poza środkami przewidzianymi w wariancie nr 2, doprowadziłoby do **maksymalnego ograniczenia różnic miedzy państwami członkowskimi**. Jednak państwa członkowskie mogą nie wykazać się wystarczającą elastycznością, by uwzględnić specyfikę poszczególnych państw.

Całkowite zniesienie wymogu zgłoszeń – z wyjątkiem uprzedniej kontroli – znacznie uprościłoby środowisko regulacyjne i zmniejszyło obciążenie administracyjne.

Ustanowienie Agencji Ochrony Danych UE znacznie zwiększyłoby **spójność egzekwowania** i usunęło nieścisłości w przypadkach, w których istnieje wyraźny wymiar unijny, lecz uprawnienia takiej agencji UE mogłyby pójść znacznie dalej na mocy przepisów prawa UE. Byłoby to jednak bardzo kosztowne dla budżetu UE. Zharmonizowane kary kryminalne także przyczyniłyby się do spójniejszego egzekwowania, lecz również one spotkałyby się z ostrym sprzeciwem państw członkowskich.

Prawa podmiotów danych. w tym prawa dzieci, także zostałyby wzmocnione, na przykład poprzez rozszerzenie definicji danych wrażliwych tak, by objąć dane dzieci oraz dane biometryczne i finansowe. Wprowadzenie prawa do „składania pozwów zbiorowych" mogłoby umożliwić maksymalizację praw na drodze sądowej. Dalszego wzmocnienia praw osób fizycznych można by oczekiwać w wyniku harmonizacji poziomu nakładanych sankcji, w tym karnych, na szczeblu UE.

Wyraźne zmiany we wszystkich instrumentach rozszerzające ogólne zasady ochrony danych na obszar współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych miałyby pozytywny wpływ, jeśli chodzi o spójność i zgodność przepisów w tym obszarze oraz wzmocnienie praw osób fizycznych. Takie radykalne podejście napotkałoby jednak opór ze strony państw członkowskich i byłoby trudne do osiągnięcia ze względów politycznych.

7. PORÓWNANIE WARIANTÓW

Wariant polityki nr 1 prowadziłby do mniejszego poziomu zgodności i kosztów administracyjnych, zwłaszcza dla prywatnych administratorów danych, gdyż większość dodatkowych kosztów obciążałaby krajowe i unijne organy publiczne. Jednocześnie miałby on jednak wyłącznie **ograniczony pozytywny wpływ na zidentyfikowanie problemy i osiągnięcie celów polityki**.

Jeśli chodzi o wykonalność polityczną, chociaż propozycje te nie budzą kontrowersji, ten wariant polityki prawdopodobnie napotka opór zainteresowanych podmiotów ze względu na ograniczony zakres i wpływ na problemy, i nie zostanie uznany na wystarczająco ambitny.

Wariant polityki nr 2 doprowadzi do **istotnego zmniejszenia rozdrobnienia i niepewności prawnej**. Można oczekiwać, że będzie mieć większy wpływ na rozwiązanie zidentyfikowanych problemów i osiągnięcie celów polityki. Równowaga między zapewnieniem zgodności a **kosztami administracyjnymi związanymi z tym wariantem polityki wydaje się rozsądna z punktu widzenia korzyści i oszczędności w wysokości około 2,3 mld EUR, jeśli chodzi o obciążenie administracyjne w ciągu roku, co będzie miało duże znaczenie dla przedsiębiorstw**. Ogólnie rzecz ujmując, wariant ten zapewni lepsze i spójniejsze egzekwowanie. Zniesienie obowiązku zgłoszeń na rzecz prostszego „systemu podstawowej rejestracji" także uprościłoby otoczenie regulacyjne i zmniejszyło obciążenie administracyjne.

Jeśli chodzi o akceptację zainteresowanych podmiotów, wariant ten byłby ogólnie dobrze przyjęty przez podmioty gospodarcze i organy publiczne, gdyż zmniejszałby koszty zapewnienia zgodności, zwłaszcza te związane z obecnym rozdrobnionym systemem. Wzmocnienie praw ochrony danych spotkałoby się z pozytywnym przyjęciem ze strony społeczności ochrony danych, w szczególności organów ds. ochrony danych. Jeśli chodzi o trzeci cel ogólny, wariant ten przyczyniłby się do osiągnięcia celów polegających na zapewnieniu **większej spójności i zgodności przepisów dotyczących ochrony danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych** poprzez uchylenie decyzji ramowej i dostosowanie jej do traktatu lizbońskiego, eliminując w ten sposób występujące w niej luki, zwłaszcza poprzez rozszerzenie jej zakresu na przetwarzanie na szczeblu krajowym.

Wariant polityki nr 3 obejmuje większość środków przewidzianych w wariancie polityki nr 2, chociaż pod kilkoma względami jest bardziej dalekosiężny. Miałby zatem **duży i pozytywny wpływ, zarówno jeśli chodzi o obniżenie kosztów związanych z rozdrobnieniem prawnym, jak i wzmocnienie praw osób fizycznych**. Ponadto zmaksymalizowałby spójność i zgodność przepisów dotyczących ochrony danych w poprzednim trzecim filarze i podniósłby standardy ochrony danych w tym kontekście. Niektóre środki objęte tym wariantem wiązałyby się jednak albo ze **zbyt wysokimi kosztami zapewnienia zgodności albo prawdopodobnie napotkałyby silny opór zainteresowanych podmiotów**. Ponadto

jednoczesna zmiana wszystkich instrumentów z poprzedniego trzeciego filara byłaby bardzo skomplikowania i kontrowersyjna ze względów politycznych.

Preferowany wariant:

Preferowany wariant to wariant nr 2 w połączeniu:

– ze zniesieniem obowiązku zgłaszania przewidzianego w wariancie nr 3, oraz

– z kilkoma „miękkimi środkami" przewidzianymi w wariancie nr 1: promowaniem korzystania z technologii zwiększających ochronę prywatności oraz systemami certyfikacji.

Preferowany wariant to wariant, który najbardziej prawdopodobnie przyczyni się do ociągnięcia celów polityki bez konieczności ponoszenia nadmiernych kosztów zapewnienia zgodności, przy istotnym zmniejszeniu obciążenia administracyjnego.

Wzmocnione przepisy dotyczące ochrony danych będą prawdopodobnie wiązać się z dodatkowymi kosztami zapewnienia zgodności, zwłaszcza jeśli chodzi o administratorów przeprowadzających ryzykowne operacje przetwarzania danych. Jednak stabilny system ochrony danych może oferować gospodarce UE przewagę konkurencyjną, gdyż wyższy poziom ochrony i przewidywana mniejsza liczba incydentów związanych z ochroną danych i naruszeń tej ochrony mogą zwiększyć zaufanie konsumentów. Wymóg nakładany na przedsiębiorstwa, by przyjmowały wysokie standardy ochrony danych może także prowadzić do poprawy sytuacji przedsiębiorstw europejskich w perspektywie długoterminowej, gdyż mogłyby się one stać światowymi liderami w technologii zwiększającej ochronę prywatności lub rozwiązaniach w zakresie ochrony prywatności już w fazie projektowania, przyciągając przedsiębiorstwa, pracowników i kapitał do Unii Europejskiej.

Ponadto w przypadku przedsiębiorstw działających na rynku wewnętrznym UE większa harmonizacja spowoduje, że transgraniczne przetwarzanie danych będzie łatwiejsze i tańsze. To z kolei powinno istotnie zachęcić te przedsiębiorstwa do rozwijania swojej działalności za granicą i czerpania korzyści z rynku wewnętrznego, co przyniesie korzystne skutki zarówno dla konsumentów, jak i gospodarki europejskiej jako całości.

Preferowany wariant obejmuje zrównoważone rozwiązane także jeśli chodzi o problem nr 3, gdyż wzmacnia prawa osób fizycznych, eliminuje luki i zmniejsza nieścisłości w zakresie ochrony danych w obszarze współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, przy jednoczesnym uproszczeniu współpracy w zakresie egzekwowania prawa i respektowaniu specyfiki sektora oraz jego potrzeb operacyjnych.

8. MONITOROWANIE I OCENA

Monitorowanie i ocena wpływu preferowanego wariantu będą opierać się przede wszystkim na takich elementach jak: korzystanie z nowych instrumentów wprowadzonych przez reformę, uprawnienia i zasoby krajowych organów ds. ochrony danych, sankcje nakładane za naruszenie przepisów dotyczących ochrony danych, czas i koszty poniesione przez administratorów danych na zapewnienie zgodności oraz zwiększenie zaufania osób fizycznych do ochrony ich danych osobowych w środowisku internetowym.