

Grupa Robocza ds. Policji i Wymiaru Sprawiedliwości

Katalog ochrony danych w zakresie współpracy i nadzoru w obszarze egzekwowania prawa w Europie

Przyjęty przez WPPJ dnia 24 marca 2009 r.

I. Wstęp

Zgodnie z artykułem 1.1 Regulaminu Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości (dalej zwanej WPPJ) *Europejska Konferencja organów ochrony danych wyznaczyła WPPJ zadanie monitorowania i badania wydarzeń w obszarze policji i egzekwowania prawa w celu sprostania wyzwaniom ochrony osób w zakresie przetwarzania ich danych osobowych.*

Jak stwierdzono w tzw. inicjatywie londyńskiej „Ochrona danych może stać się rzeczywistością tylko wówczas, gdy zasady ochrony danych będą przestrzegane w praktyce. Organy ochrony danych mają do odegrania kluczową rolę w zapewnieniu zgodności, ale uda im się to jedynie, gdy będą skutecznie przekazywać komunikaty na temat ochrony danych i zaangażują w to zadanie innych interesariuszy oraz, gdy to konieczne, będą efektywnie wykorzystywać swoje uprawnienia w zakresie dochodzeń i egzekwowania”.

Oceniając wydarzenia w obszarze egzekwowania prawa, europejskie organy ochrony danych kilkakrotnie podkreślały potrzebę skutecznego nadzoru w obszarze egzekwowania prawa.¹

Już na Konferencji w Budapeszcie w 2006 r. europejskie organy ochrony danych wyznaczyły poprzednikowi WPPJ – Grupie Roboczej ds. Policji – zadanie opracowania ujednoliconych instrumentów w zakresie metod kontroli i inspekcji.

W wyniku już trwających prac, we wrześniu 2007 r. WPPJ postanowiła zbadać możliwości zwiększenia skuteczności nadzoru (inspekcji i interwencji) oraz opracować wspólną politykę nadzoru dla europejskich organów ochrony danych.

Ponadto uznaje się, że wydarzenia w Unii Europejskiej mające na celu zwiększenie współpracy między organami wymiaru sprawiedliwości poprzez zachęcanie do wymiany danych osobowych może spowodować dodatkowe obciążenie dla osoby, której dane dotyczą, przy korzystaniu z praw podstawowych. Za konieczne uważa się zwiększenie współpracy między krajowymi organami ochrony danych w zakresie pomocy dla osób, których dane dotyczą.

Dokument WPPJ zapewnia katalog dla współpracy w różnych obszarach związanej z podstawowym zadaniem nadzoru. Zawiera także przegląd wspólnych podejść do różnych tematów związanych z zadaniami krajowych organów ochrony danych i WPPJ.

¹ Patrz np. stanowisko Wiosennej Konferencji dot. egzekwowania prawa i wymiany informacji (Kraków, 25-26 kwietnia 2005 r.), opinia tej konferencji dot. decyzji ramowej w sprawie ochrony danych (Bruksela, 24 stycznia 2006 r.) oraz Opinia 3/2006 GR Art. 29 w sprawie Dyrektywy 2006/24/WE.

II. Uwagi ogólne

WPPJ opracowała kwestionariusz w celu zgromadzenia informacji dotyczących kompetencji organów ochrony danych w Państwach Członkowskich w zakresie nadzoru nad organami wymiaru sprawiedliwości. Otrzymane odpowiedzi stanowiły podstawę do znalezienia wspólnych podstaw do zachęcania do prowadzenia polityki w zakresie nadzorowania działań związanych z egzekwowaniem prawa. Biorąc pod uwagę ciągły wzrost wymiany informacji w Unii Europejskiej przyjmującej różne formy gromadzenia informacji i ich udostępniania oraz działania w zakresie dalszej harmonizacji ochrony danych w przypadku egzekwowania prawa, taka wspólna polityka stanowi logiczną odpowiedź dotyczącą ochrony danych, która wzmacnia rolę krajowych organów ochrony danych oraz daje wspólną odpowiedź na możliwe (nowe) wyzwania.

WPPJ wykorzystała także informacje zgromadzone w 2006 r. dzięki kwestionariuszowi dotyczącemu praw osób, których dane dotyczą, oraz przetwarzania danych przez organy policji. Informacje te pomogły WPPJ w opracowaniu zasad współpracy stanowiących pomoc dla osób, których dane dotyczą, w wykonywaniu ich praw w sytuacjach, gdy informacje są przetwarzane w innym państwie lub w więcej niż jednym państwie członkowskim.

Współpraca bez wątpienia przyczyni się do lepszego zrozumienia tego, jak należy poprawić skuteczność nadzoru. W związku z tym różne obszary współpracy opisane w tym katalogu są przedmiotem okresowej oceny.

III. Skuteczny nadzór

Artykuł 29 TEU (Traktatu o Unii Europejskiej) ma na celu zapewnienie obywatelom wysokiego poziomu bezpieczeństwa w obszarze wolności, bezpieczeństwa i wymiaru sprawiedliwości. Ten obszar wolności, bezpieczeństwa i wymiaru sprawiedliwości stopniowo się rozwija i prowadzi do zniesienia granic między państwami członkowskim oraz do swobodnego przepływu informacji z zakresu egzekwowania prawa.

Wzrost współpracy w zakresie egzekwowania prawa, stwierdzenie, że współpraca w tym zakresie nie jest ograniczona przez granice krajowe oraz istniejące platformy służące tej współpracy (Europol, Eurojust, Schengen, Prüm²), zmuszają krajowe organy ochrony danych oraz wspólne organy zajmujące się nadzorem do zainwestowania w opracowanie wspólnego podejścia dotyczącego nadzorowania przetwarzania danych związanych z egzekwowaniem prawa.

W 2005 r. europejskie organy ochrony danych już zadeklarowały, że *„Zważywszy na zobowiązanie Unii do poszanowania praw człowieka i podstawowych wolności, należy wprowadzić inicjatywy na rzecz poprawy egzekwowania prawa w UE, takie jak zasada dostępności, na podstawie odpowiedniego systemu porozumień o ochronie danych gwarantujących wysoki i równoważny standard ochrony danych”*.³

Zasada „dostępności” mająca na celu ułatwienie zwalczania przestępczości może stworzyć elastyczną infrastrukturę umożliwiającą organom wymiaru sprawiedliwości dostęp do danych dostępnych w innych państwach członkowskich bez żadnych przeszkód prawnych ani technicznych.

Poprawa możliwości egzekwowania prawa w celu zwalczania terroryzmu i innych poważnych przestępstw musi być połączona z poszanowaniem praw podstawowych. *Ochrona i poszanowanie* powinny być kluczowymi słowami mającymi na celu osiągnięcie obu celów. Należy utrzymać odpowiednią równowagę między celem w postaci zapewnienia wysokiego poziomu bezpieczeństwa ludzi oraz celem, jakim jest ochrona praw podstawowych. Organy ochrony danych powinny odegrać aktywną rolę w tym procesie.

² Decyzja Rady w sprawie intensyfikacji współpracy transgranicznej, w szczególności w zwalczaniu terroryzmu i przestępczości transgranicznej.

³ Deklaracja Krakowska, 25-26 kwietnia 2005 r.

Sam nadzór obejmuje szereg działań, które krajowe organy ochrony danych mogłoby przeprowadzić, w tym konsultacje, podnoszenie świadomości, propagowanie ochrony danych wśród ogółu, etc.

Jeżeli chce się odpowiedzieć na nowe trendy odzwierciedlone w nowych inicjatywach Unii Europejskiej dotyczących przetwarzania danych osobowych przez organy wymiaru sprawiedliwości oraz jednocześnie zwiększyć interoperacyjność europejskich baz danych, konieczne jest zapewnienie bardziej skutecznego i wiarygodnego nadzoru nad ochroną danych w UE.

Potrzeba i znaczenie współpracy i wspólnych działań krajowych organów ochrony danych w 3 filarze UE podkreślono ustanawiając wspólne organy nadzorcze, takie jak Wspólny Organ Nadzorczy Schengen, Wspólny Organ Nadzorczy Europolu, Wspólny Organ Nadzorczy Eurojust, Wspólny Organ Nadzorczy ds. Celnych, w celu zapewnienia wspólnej niezależnej kontroli i nadzoru nad przetwarzaniem danych w 3 filarze oraz ochrony praw osób fizycznych.

Nawet jeżeli Traktat z Lizbony zmieniający istniejące traktaty UE wejdzie w życie, nie zmieni to potrzeby takiej współpracy.

Aspekt zwiększonego nadzoru i współpracy między organami ochrony danych staje się jeszcze ważniejszy w sytuacji, gdy informacje związane z egzekwowaniem prawa „będą podlegały wymianie”/„będą udostępniane” zgodnie z zasadą „dostępności” w tym samym czasie przez organy w różnych państwach członkowskich. Oznacza to, że przetwarzanie w kilku jurysdykcjach będzie uregulowane różnymi krajowymi przepisami i ze względu na brak kompetencji w innych jurysdykcjach oraz różnice kompetencyjne krajowe organy ochrony danych będą musiały liczyć na pomoc krajowych organów ochrony danych z poszczególnych państw członkowskich.

W związku z tym zainwestowanie we wspólne podejście oparte na wspólnej polityce bez wątpienia będzie miało pozytywny wpływ na skuteczność nadzoru zarówno na poziomie krajowym, jak i międzynarodowym.

W niektórych obszarach metodologia wspólnych inspekcji już jest rozwijana i wykorzystywana przez krajowe organy ochrony danych. Doświadczenie w zakresie wspólnych inspekcji dotyczących wykorzystania systemu informacyjnego Schengen, skoordynowana inspekcja Eurodac, wspólne inspekcje w Eurojust i Europolu oraz inicjatywy podejmowane przez Wspólny Organ Nadzorczy Europolu są przykładem wartości dodanej wspólnego podejścia.

W kierunku polityki wspólnego nadzoru

Podczas posiedzenia w październiku 2007 r. WPPJ postanowiła zbadać możliwości opracowania europejskiej polityki ochrony danych w zakresie nadzoru nad przetwarzaniem danych przez organy wymiaru sprawiedliwości. W ramach pierwszego kroku naprzód WPPJ przeanalizowała obecne zadania krajowych organów ochrony danych. Na podstawie otrzymanych odpowiedzi na kwestionariusz „Kompetencje organów ochrony danych w obszarze egzekwowania prawa” ustalono, że wszystkie europejskie organy ochrony danych posiadają kompetencje w tym obszarze, w tym kompetencje w zakresie nadzorowania przetwarzania danych prowadzonego przez organy wymiaru sprawiedliwości. Odpowiedzi na kwestionariusz pokazują również, że większość europejskich organów ochrony danych posiada specjalną (strategiczną) politykę przyjętą w celu przeprowadzania inspekcji/audytów, która jest także wykorzystywana w obszarze egzekwowania prawa.

Następnym niezbędnym warunkiem do rozwinięcia skutecznego nadzoru jest metodologia stosowana przez krajowe organy ochrony danych przy przeprowadzaniu inspekcji. I w tym przypadku wyniki kwestionariusza są pozytywne: 18 krajowych organów ochrony danych już stosuje specjalną metodologię audytową.

Wyniki ewidentnie wskazują, że nadzór oparty na specjalnej polityce już stanowi licznie popierane podejście, co jest istotnym argumentem za opracowaniem wspólnej polityki.

Przy opracowywaniu takiej wspólnej polityki najpierw należy wykryć zagrożenia dla ochrony danych przy egzekwowaniu prawa oraz je zaklasyfikować wedle wpływu tych zagrożeń. Ocena ryzyka pomoże w określeniu niezbędnych odpowiedzi na te zagrożenia.

Należy koniecznie zauważyć, że zagrożenia nie są ograniczone do przetwarzania danych w środowisku zajmującym się egzekwowaniem prawa. Gromadząc i wykorzystując te dane, organy wymiaru sprawiedliwości są w kontakcie z innymi podmiotami, zarówno w sektorze publicznym, jak i prywatnym, co może stworzyć określone zagrożenia dla ochrony danych.

Ocena ryzyka

EGZEKWOWANIE PRAWA

Przed rozpoczęciem oceny ryzyka należy określić obszar, jaki będzie przedmiotem oceny. Mimo że wyrażenie „egzekwowanie prawa” (law enforcement) stanowi pierwszą wskazówkę, samo w sobie jest zbyt niejasne, aby przedstawiało wyraźnie zakreślony obszar oceny. Organy wymiaru sprawiedliwości działają w złożonym środowisku i mają różne zadania, takie jak: zapobieganie przestępczości i jej wykrywanie, dochodzenia, edukacja, szkolenia,

egzekwowanie przepisów, bezpieczeństwo, kontrola ruchu oraz funkcje w zakresie bezpieczeństwa publicznego. Ponadto różnice w przepisach krajowych i politykach krajowych poszczególnych państw członkowskich oraz wynikające z tego różnice w realizacji tych zadań przez organy wymiaru sprawiedliwości uniemożliwiają opracowanie instrumentu oceny ryzyka uwzględniającego wszystkie aspekty różnych zadań objętych terminem egzekwowanie prawa. W celu przeprowadzenia oceny ryzyka, która będzie pomocna przy opracowaniu polityki nadzoru, konieczne będzie określenie niektórych parametrów definiujących konkretny obszar oceny.

W tym celu wykorzystuje się następującą definicję obszaru, który ma być oceniany:

Wszystkie działania w zakresie przetwarzania danych prowadzone przez organy wymiaru sprawiedliwości, które uznaje się za ich podstawową działalność i które mają na celu zapobieganie, wykrywanie, prowadzenie dochodzeń oraz ściganie przestępstw lub ochronę bezpieczeństwa publicznego.

Taka definicja pozwala na pewną elastyczność potrzebną do poradzenia sobie z krajowymi różnicami w rodzajach organizacji wymiaru sprawiedliwości oraz obejmuje wszystkie publiczne, a nawet prywatne organizacje, których zadaniem prawnym może być zwalczanie przestępczości.

WSKAŹNIKI RYZYKA

W celu wykrycia, czy określone działania mogą stanowić określone zagrożenia dla ochrony danych, konieczne jest opracowanie zestawu wskaźników, które mogą pomóc w wyborze priorytetów nadzorczych dla organów ochrony danych. Wskaźniki te mogą również pomóc w opracowaniu polityki nadzoru.

Brakuje przykładów istniejących konkretnych wskaźników ryzyka wykorzystywanych w celu opracowania polityki nadzoru w obszarze egzekwowania prawa. Jednakże różne istniejące ogólne metody oceny wpływu na prywatność (PIA) obejmują cenne aspekty, które można wykorzystać przy tworzeniu konkretnego zestawu wskaźników ryzyka, typowych dla określonego obszaru egzekwowania prawa.

Biorąc pod uwagę obszar, który ma być poddany ocenie, oraz specyficzny charakter zadania i metod działania organów egzekwowania prawa, wskaźniki ryzyka dzieli się na cztery kategorie: kategoria danych, kategoria osób, rodzaj przetwarzania oraz rodzaj działań z zakresu egzekwowania prawa.

Kategoria danych

Procesy biznesowe w organizacjach wymiaru sprawiedliwości obejmują przetwarzanie kategorii danych, które można rozróżnić wedle ich funkcji w procesie, wedle fazy przetwarzania informacji w dochodzeniu oraz wedle ich treści. Takie rozróżnienie jest niezbędne do umożliwienia właściwej oceny wszelkich zagrożeń związanych z przetwarzaniem tych danych. Należy zauważyć, że rozróżnienie dokonane między kategoriami danych i nazw wykorzystywanych do opisanie tych kategorii może różnić się od tego, co jest praktykowane w niektórych krajach.

Dane twarde (hard data)

Słowo „twarde” wskazuje, że ta kategoria danych odnosi się do danych, które są lub mogą być obiektywnie określone. Obejmują one szereg danych, począwszy od opisu faktu (transakcja finansowa miała miejsce, osoba została dostrzeżona na obrazach z kamery przemysłowej, dane dochodzeniowe), poprzez oświadczenie podejrzanego, ofiary lub świadka bądź innych osób w formie oficjalnego zapisu (procès-verbal), po zapisany wynik ostateczny dochodzenia i/lub oficjalną decyzję sądu lub prokuratury.

Dane miękkie (soft data)

Dane miękkie obejmują wszystkie inne zebrane informacje, które mają być wykorzystane do oceny i analizy w trakcie dochodzenia. W praktyce istnieje wiele różnych interpretacji tego, co uważa się za dane miękkie, ale aby móc dokonać rozróżnienia między wszystkimi danymi, które mogą być wykorzystane przez organy wymiaru sprawiedliwości, dane miękkie to w praktyce wszystkie dane, które nie są objęte kategorią danych twardych.

Dane szczególnie chronione (wrażliwe)

We wszystkich właściwych przepisach o ochronie danych dane szczególnie chronione uznaje się za kategorię danych, do których należy stosować szczególne zasady. Charakter tych danych oraz określonych zagrożeń przy przetwarzaniu tych danych uzasadniają fakt, że ta kategoria danych jest również wskazana jako szczególny wskaźnik ryzyka. Należy zauważyć, że niektóre dane szczególnie chronione mogą również mieścić się w definicji danych twardych (np. odciski palców, DNA). Jednakże gdy dane szczególnie chronione są częścią przetwarzania informacji, należy zawsze stosować wskaźnik ryzyka dla danych szczególnie chronionych.

Kategoria osób

Organizacja wymiaru sprawiedliwości zaangażowana w wykrywanie, prowadzenie dochodzeń lub ściganie przestępstw lub ochronę bezpieczeństwa publicznego przetwarza dane różnych kategorii osób.

Podjejrzeni

Jeżeli chodzi o źródła informacji wykorzystywane przez organy wymiaru sprawiedliwości, przetwarzane są dane podejrzanych, świadków, ofiar i innych powiązanych osób, osób przesłuchiowanych lub osób, które dostarczają informacje. Generalnie podczas wszystkich dochodzeń doraźnych (re-active) i niektórych dochodzeń prewencyjnych (pro-active) są przetwarzane dane tych kategorii osób. Nie wykorzystuje się danych dotyczących świadków i ofiar w celu oceny ryzyka.

Niepodjejrzeni

Szczególną uwagę należy zwrócić na tzw. dochodzenia prewencyjne, ponieważ towarzyszy im przetwarzanie danych dotyczących osób nie ze względu na ich udział w przestępstwie, ale ze względu na ich przynależność do określonej grupy lub gdy z innego względu dotyczące ich dane uważa się za przydatne. Przetwarzanie danych tej kategorii niepodjerzanych ewidentnie stanowi zagrożenie.

Rodzaj przetwarzania

Standardowy proces biznesowy organizacji wymiaru sprawiedliwości składa się z gromadzenia i analizowania danych oraz ich przetwarzania. Samo w sobie nie będzie to powodem do stworzenia odrębnego wskaźnika ryzyka dla ogólnego przetwarzania danych.

Zbiory analityczne

Jednakże szczególnie w procesie analizy istnieje wyraźna tendencja do kompilowania danych z różnych źródeł i spraw w specjalne zbiory danych (takie jak hurtownie danych) w celach analitycznych. Ze względu na fakt, że taka analiza realizowana jest w sposób, który często nie jest monitorowany oraz na wpływ, jaki może to mieć na poszczególne osoby, zwłaszcza w połączeniu z wyszukiwaniem danych oraz hurtowniami danych, może to uzasadniać wniosek, że jest to postrzegane jako realne zagrożenie dla osób.

Tworzenie profili

Jednym z charakterystycznych aspektów analizy kryminalnej jest tworzenie profili. Istnieją różne przyczyny wykorzystywania jako instrumentu dochodzeniowego tworzenia profili i istnieją różne metody tworzenia profili. Najbardziej znane to tworzenie profili przestępców oraz tworzenie profili etnicznych – metody stosowane przez organy wymiaru sprawiedliwości. W zależności od rodzaju tworzenia profili, wykorzystywanych danych oraz rodzaju działania z zakresu egzekwowania prawa, może stwarzać to określone zagrożenia dla ochrony danych, które uzasadniają wykorzystanie tworzenia profili jako odrębnego wskaźnika ryzyka.

Interoperacyjność

Program Haski kładzie silny nacisk na wymianę informacji przy zastosowaniu zasad, takich jak zasada dostępności i interoperacyjności. Systemy informacyjne na poziomie krajowym oraz na poziomie UE powinny wykorzystywać nową technologię w celu zwiększenia wymiany informacji. W przypadku, gdy zasada „dostępności” może spowodować określone zagrożenia dla ochrony danych (zmiana celu, czyli tzw. function creep, naruszenie zasady ograniczenia celu), nie jest wystarczająca szczegółowa, aby można ją było wykorzystać jako wskaźnik ryzyka. Ponadto środowisko ochrony danych już opracowało instrument do oceny wszelkich propozycji stworzenia lub zwiększenia dostępności danych do celów egzekwowania prawa.⁴

Interoperacyjność systemów informatycznych może stwarzać szczególne zagrożenia dla ochrony danych, na przykład poprzez wykorzystanie jednego zestawu danych w celu zidentyfikowania danych dotyczących konkretnej osoby w różnych systemach. Wywołuje również pytania o niezbędne poziomy jakości danych wykorzystywane w różnych systemach, które staną się systemami interoperacyjnymi. Interoperacyjność jest zatem postrzegana jako wskazanie określonego zagrożenia, ale poziom zagrożenia zależy od istnienia innych wskaźników ryzyka.

Wymiana międzynarodowa (przekazywanie transgraniczne)

Dane związane z egzekwowaniem prawa podlegają wymianie na terytorium UE na poziomie dwu- lub wielostronnym, ze zbiorami danych UE lub z krajami trzecimi lub organizacjami. Niekoniecznie stwarza to określone zagrożenie dla ochrony danych, jednakże w odniesieniu do istnienia innych wskaźników ryzyka może powodować to dodatkowe ryzyko.

⁴ Wspólne stanowisko w sprawie dostępności, Larnaka 10-11 maja 2007 r.

Przekazywanie transgraniczne jako wskaźnik ryzyka koncentruje się na potrzebie posiadania zabezpieczeń w celu kontroli wymiany danych, aby zapewnić wysoki i trwały poziom jakości danych oraz system służący wzajemnemu informowaniu się o wszelkich zmianach danych. Uzasadnia to wykorzystanie go jako wskaźnika ryzyka.

Rodzaj działań z zakresu egzekwowania prawa

Generalnie działania z zakresu egzekwowania prawa można rozróżnić na działania doraźne i prewencyjne. W szczególności działania prewencyjne, w zależności od wykorzystywanych danych, metody działania (na przykład tworzenie profili) oraz wykorzystania wyników działalności, stwarzają szczególne zagrożenie dla ochrony danych. Rodzaj działania z zakresu egzekwowania prawa jako wskaźnik ryzyka jest niezbędny do dokonania oceny, czy inne istniejące potencjalne zagrożenia, które mogą nie uzasadniać wspólnego podejścia, uzasadniają takie podejście przy połączeniu z konkretnym działaniem z zakresu egzekwowania prawa.

OCENA RYZYKA

Te wskaźniki ryzyka mają celu pomóc organom ochrony danych stwierdzić, czy określone działania w zakresie przetwarzania danych mogą stwarzać takie zagrożenia wymagające skutecznego i wspólnego nadzoru. Istnienie określonego połączenia wskaźników ryzyka może doprowadzić do oceny uznającej działanie za uzasadnione.

Umieszczenie wszystkich wskaźników ryzyka we wzorcu i dokonanie oceny działań z zakresu egzekwowania prawa przy wykorzystaniu tego wzorca może pomóc organom ochrony danych w opracowaniu polityki wspólnego nadzoru.

| | Zbiory analityczne | Tworzenie profili | Interoperacyjność | Przekazywanie transgraniczne | Działanie prewencyjne |
|----------------------------|--------------------|-------------------|-------------------|------------------------------|-----------------------|
| Dane twarde | | | | | |
| Dane miękkie | | | | | |
| Dane szczególnie chronione | | | | | |
| Podejrzani | | | | | |
| Niepodejrzani | | | | | |

Podanie, czy wskaźnik ryzyka ma zastosowanie przy ocenie określonych działań z zakresu egzekwowania prawa związanych z przetwarzaniem danych pomoże w wyborze działań, które wymagają bliższego przyjrzenia się im przez organy ochrony danych.

Na przykład zastosowanie następujących wskaźników ryzyka

| | Zbiory analityczne | Tworzenie profili | Interoperacyjność | Przekazywanie transgraniczne | Działanie prewencyjne |
|----------------------------|--------------------|-------------------|-------------------|------------------------------|-----------------------|
| Dane twarde | | | | | |
| Dane miękkie | | | | x | |
| Dane szczególnie chronione | | x | | | x |
| Podejrzani | | | | | |
| Niepodejrzani | | x | | | x |

uzasadni wspólne działanie przy porównaniu z

| | Zbiory analityczne | Tworzenie profili | Interoperacyjność | Przekazywanie transgraniczne | Działanie prewencyjne |
|----------------------------|--------------------|-------------------|-------------------|------------------------------|-----------------------|
| Dane twarde | x | | | x | |
| Dane miękkie | x | | | | |
| Dane szczególnie chronione | | | | | |
| Podejrzani | | | | | |
| Niepodejrzani | | | | | |

Polityka wspólnego nadzoru

Przy opracowywaniu polityki wspólnego nadzoru konieczne będzie połączenie motywów stworzenia takiej polityki z oczekiwanym rezultatem tej polityki oraz możliwościami i instrumentami służącymi osiągnięciu takich wyników.

Jak już wspomniano, wzrost współpracy w zakresie egzekwowania prawa, tendencja do udostępniania danych oraz konieczność doprowadzenia do interoperacyjności systemów zmusza środowisko ochrony danych do zainwestowania we wspólne podejście, nie tylko poprzez określenie wspólnych celów, ale również przez wykorzystanie tych samych metod inspekcji i sprawozdawczości pozwalającej na odpowiednie porównania. Rozdział IV tego katalogu przedstawia niezbędne moduły ujednoliconych metod inspekcji.

Wynikiem takiego działania będzie lepsze zrozumienie tego, co się dzieje w praktyce oraz gdzie należy podjąć dalsze działania, w tym wspólne stanowiska. Następnym ważnym wynikiem jest fakt, że nadzór w rzeczywistości ma miejsce, co może zapewnić skutek prewencyjny.

Wspólna europejska polityka nadzoru nie powinna być odczuwana jako rygorystyczny instrument obejmujący wszystkie możliwe zagrożenia oraz zobowiązujący wszystkie europejskie organy ochrony danych do działania. W sytuacji, gdy zagrożenia uznaje się za wymagające wspólnego podejścia, wspólna polityka nadzoru bierze pod uwagę fakt, że zagrożenia te nie mogą istnieć we wszystkich państwach europejskich, a także przyznaje, że nie zawsze wszyscy mają możliwość działania. Priorytety krajowe lub ograniczenia praktyczne mogą ograniczyć wkłady europejskich organów ochrony danych. Wspólna polityka nie prowadzi automatycznie do podejmowania działań przez wszystkich: ma na celu stworzenie wspólnego zrozumienia znaczenia kontroli w określonych obszarach oraz wyraźnej intencji działania.

Uwzględniając cykl życia polityki,

Wybór celów

Ocena ryzyka

Nadzór

Ocena i zalecenia

można przedstawić następujący opis wspólnej polityki nadzoru określającej cele okresowe:

Europejskie organy ochrony danych powinny okresowo podejmować decyzję, jakie rodzaje przetwarzania danych lub działania w zakresie przetwarzania danych w obszarze egzekwowania prawa będą przedmiotem skutecznej inspekcji. Wyniki tych inspekcji należy udostępnić i ocenić, a gdy to konieczne, należy opracować wspólne zalecenia. Europejska Konferencja Organów Ochrony Danych powinna w wyniku propozycji WPPJ co dwa lata opracowywać wspólną politykę nadzoru.

Przy opracowywaniu takiej polityki określającej konkretne cele na najbliższe dwa lata istotne są następujące kroki:

Ocena ryzyka i wybór celów

Każdy członek WPPJ zobowiązany jest do oceny działań w zakresie przetwarzania danych prowadzonych przez organy wymiaru sprawiedliwości w ich poszczególnych krajach, przy wykorzystaniu metody oceny ryzyka, opisanej w tym rozdziale. Wspólne organy nadzorcze powinny wykorzystywać tę samą metodę przy wyborze określonych zagrożeń dla ochrony danych w ich organizacjach i/lub we współpracy z i między państwami.

Wyniki tej oceny należy przedstawić WPPJ, która, na podstawie zagrożeń dla ochrony danych, wybierze te działania z zakresu przetwarzania, które należy poddać inspekcji i ocenie w ciągu najbliższych dwóch lat. Wybór ten powinien być ograniczony, aby pozwolić zaangażowanym członkom na rzeczywiste przeprowadzenie inspekcji oraz na przedstawianie WPPJ sprawozdań w okresie dwóch lat.

WPPJ zobowiązana jest do przedstawienia propozycji do przyjęcia Europejskiej Konferencji Organów Ochrony Danych.

Nadzór

Inspekcje należy przeprowadzać zgodnie z metodami inspekcji opisanymi w rozdziale IV. W zależności od zagrożeń, WPPJ może podjąć decyzję o konkretnej metodzie inspekcji. W zależności od celu inspekcji i zagrożeń, będzie opracowany model sprawozdawczy pozwalający organom ochrony danych na przedstawianie wyników inspekcji WPPJ. Pomoże to WPPJ porównać wyniki oraz jednocześnie zapobiec przekazywaniu konkretnych wyników inspekcji, które są istotne tylko dla danego kraju.

Ocena i zalecenia

Sprawozdania z inspekcji pomogą europejskim organom ochrony danych w dalszej ocenie zagrożeń oraz przygotowaniu rozwiązań. Na podstawie takiej oceny WPPJ może zaproponować dalsze działania i/lub zalecenia Europejskiej Konferencji.

Porównanie ustaleń i wstępnej oceny ryzyka zostanie wykorzystane także do oceny metody oceny ryzyka.

IV. Ujednolicenie metod inspekcji

Niezbędnym zadaniem wszystkich organów ochrony danych jest nadzorowanie przetwarzania danych. Do celów kontroli zgodności z zasadami ochrony prywatności wiele spośród tych organów opracowało różnorodne praktyki, metody i metodologie. Dotyczą one podstawowych aspektów krajowych przepisów o ochronie danych. W badaniu WPPJ dotyczącym utworzenia struktury służącej inspekcji akt policyjnych przedstawiony jest zarys wspólnej struktury audytu ochrony prywatności dla sektora policji, z zapewnieniem, że metodologia i wyniki są porównywalne. W tym rozdziale kwestia ta przedstawiona jest dokładniej.

Audyt ochrony prywatności ma na celu sprawdzenie, czy administrator ustanowił mechanizmy zapewniające, że dane osobowe są uzyskiwane i przetwarzane rzetelnie, zgodnie z prawem oraz na odpowiedniej podstawie. Poddaje również przeglądowi odpowiedzialność administratora za jakość przetwarzanych danych, za to, aby dane były dokładne, kompletne i aktualne, adekwatne, istotne oraz nienadmierne w odniesieniu do celu. Do podstawowych celów audytu ochrony prywatności należą także inne kwestie, takie jak odpowiednie selekcjonowanie i usuwanie danych osobowych, dokumentacja autoryzowanego korzystania z systemów, np. kodeksy postępowania, wytyczne, etc., bezpieczeństwo systemów, przestrzegania praw osób, takich jak prawo dostępu osoby, której dane dotyczą.

Korzyści z opracowania audytu ochrony prywatności odnoszą nie tylko organy danych. Pomoże on także organom policji:

- zidentyfikować kwestie dotyczące niezgodności i/lub wykryć słabe strony w ich własnej strukturze zarządzania przetwarzaniem danych;
- utrzymać i zapewnić zgodność z unijnymi i krajowymi wymogami ochrony danych.

W tym rozdziale przedstawiono niezbędne kroki w kierunku opracowania struktury standardowego audytu ochrony prywatności. Nie zawiera on (jeszcze) gotowych list kontrolnych dla różnych inspekcji. W oparciu o wybory dokonane w zakresie polityki nadzoru zostanie sporządzona konkretna lista kontrolna w ramach struktury audytu ochrony prywatności, zgodnie z opisem w tym rozdziale. Takie listy kontrolne będą oceniane po ich wykorzystaniu, i jeśli wynik oceny będzie pozytywny, zostaną umieszczone w załącznikach do tego katalogu do przyszłego wykorzystania.

W kierunku struktury standardowego audytu ochrony prywatności

Standardowy program audytu ochrony prywatności powinien być przydatny dla wszystkich zaangażowanych stron (organów wymiaru sprawiedliwości oraz organów ochrony danych). Musi być również elastyczny, aby można go było dostosować do charakteru kontrolowanego administratora oraz właściwego ustawodawstwa. Ponadto program musi zapewnić standardową metodę sprawozdawczości umożliwiającą porównanie wyników audytu.

Mimo że mogą istnieć różnice w przepisach dotyczących ochrony danych poszczególnych państw europejskich, wszystkie z tych uregulowań można porównać z Konwencją nr 108, Dyrektywą UE o ochronie danych 95/46, Rekomendacją nr R87(15) oraz nową Decyzją ramową UE o ochronie danych w 3 filarze.

Struktura audytu ochrony prywatności może odnieść korzyści ze standaryzacji, pod warunkiem że wybrany zostanie format, który:

- może być stosowany przez wszystkie strony.
- jest dostosowany do międzynarodowego ustawodawstwa w zakresie ochrony danych w obszarze egzekwowania prawa, ale może być również łatwo dostosowany tak, aby spełnić dodatkowe surowe lokalne wymogi w zakresie ochrony danych.
- jest niezależny od motywu, przyczyny, zadania, celu i zakresu audytu, umożliwiając organom ochrony danych wybranie tego, na czym się chcą skupić.
- umożliwia porównanie wyników audytów mających te same założenia.

Na podstawie tej standaryzacji audyt ochrony prywatności można zdefiniować jako: systematyczne i niezależne badanie mające na celu ustalenie, czy działania obejmujące przetwarzanie danych osobowych są prowadzone zgodnie z politykami i procedurami ochrony danych obszaru egzekwowania prawa oraz, czy przetwarzanie to spełnia wszystkie wymogi prawne w zakresie ochrony danych.

Zaletą tego formatu jest fakt, że każdy organ wymiaru sprawiedliwości zaangażowany w przetwarzania danych osobowych oraz organy ochrony danych nadzorujące zgodność z przepisami, jak również oczywiście osoby, których dane dotyczą, mogą być beneficjentami standardowej struktury audytu ochrony prywatności. Ponadto, organy regulacyjne mogą wykorzystać ten format w celu uświadamiania na temat audytu ochrony prywatności oraz uproszczenia obecnej struktury regulującej kwestie ochrony prywatności.

Wprowadzenie do programu audytu ochrony prywatności

Program audytu dla egzekwowania prawa obejmuje wszystkie obszary przetwarzania danych związane z podstawową działalnością organów wymiaru sprawiedliwości. Program taki przewiduje instrumenty audytu pomagające organom ochrony danych w przeprowadzaniu audytu, przy uwzględnieniu różnych powodów audytu oraz jego celu.

Program audytu ochrony prywatności przedstawia katalog modułów audytu, które mogą być wykorzystywane niezależnie od siebie lub mogą wzajemnie się uzupełniać.

Zatem program taki powinien obejmować różne rodzaje audytu. Na podstawie oceny doświadczeń w zakresie audytu zbiorów policyjnych oraz przy uwzględnieniu różnych możliwości przeprowadzania audytu przez organy ochrony danych, można rozróżnić trzy rodzaje audytu:

Audyt adekwatności

Celem audytu adekwatności jest sprawdzenie, czy udokumentowane polityki, kodeksy postępowania, wytyczne i procedury spełniają wymogi instrumentów prawnych w zakresie ochrony danych. Audyt taki można przeprowadzić przy wykorzystaniu procedury pisemnej.

Audyt zgodności

Celem audytu zgodności jest sprawdzenie, czy organizacja rzeczywiście działa zgodnie ze swoimi udokumentowanymi politykami, kodeksami postępowania, wytycznymi i procedurami. Taki audyt zawsze przeprowadzany jest na miejscu.

Audyt na poziomie danych

Celem tego audytu jest sprawdzenie integralności (dokładności i kompletności) przetwarzanych danych osobowych. Audyt tego typu zawsze przeprowadzany jest na miejscu. Audyt taki może obejmować cały proces biznesowy w organizacji wymiaru sprawiedliwości lub dane w indywidualnej sprawie.

Należy podkreślić, że, w zależności od oceny przez organ ochrony danych potrzeby przeprowadzenia audytu, jeden audyt może zawierać elementy trzech rodzajów audytu.

Te trzy audyty zostaną opracowane w taki sposób, aby wszystkie europejskie organy ochrony danych mogły je wykorzystać.

Proces audytu ochrony prywatności

W rozdziale tym opisano fazy audytu, do których należą:

Zlecenie audytu

Przygotowanie audytu

Przeprowadzenie audytu

Audyt to systematyczne i niezależne badanie przedmiotu audytu. Proces przygotowania i przeprowadzenia audytu podzielony jest na trzy fazy.

Zlecenie audytu

Audyt jest zawsze przeprowadzany pod nadzorem organu ochrony danych i musi być oficjalnie zlecony. Zlecenie jest bardzo ważne, jest bowiem podstawą planu audytu oraz podstawą prawną działań audytora. Zlecenie musi być udokumentowane i powinno obejmować następujące elementy:

- Zleceniodawca (tj. organ ochrony danych) oraz zleceniobiorca/zleceniobiorcy (tj. audytor/audytorzy).
- Cel i charakter zlecenia (tj. poddawana audytowi organizacja wymiaru sprawiedliwości).
- Zakres audytu. Zakres przedstawiony będzie jako połączona analiza trzech podstawowych elementów. Są to cel(e), aspekt(y)⁵ oraz wymogi wynikające z zasad ochrony prywatności⁶.
- Okres, w jakim audyt będzie przeprowadzony.
- Wymagany czas i środki.
- Ograniczenia dotyczące przeprowadzenia audytu.
- Odniesienia do właściwego ustawodawstwa.

Przygotowanie audytu: plan audytu

Po ustanowieniu zlecenia, konieczne jest przygotowanie audytu poprzez opracowanie planu audytu. Plan audytu to systematyczna i zorganizowana dokumentacja działań, które muszą być zrealizowane przez audytora w celu przeprowadzenia audytu (ocena projektu systemu(ów), wdrożenie/istnienie lub skuteczność/ciągłe działanie systemu środków i procedur, które podjął administrator w celu odpowiedniej ochrony i zarządzania swoimi operacjami przetwarzania danych). Stworzenie planu audytu, który jest dostosowany do specyficznej sytuacji organizacji, jest niezbędne w celu przeprowadzenia skutecznego i wydajnego audytu. Plan audytu powinien być przyjęty przed rozpoczęciem pierwszych

⁵ Poufność, integralność, ciągłość oraz możliwość audytu.

⁶ Jakość danych, prawnie uzasadnione przetwarzanie, przejrzystość, prawa osób, których dane dotyczą, poufność i bezpieczeństwo, zgłoszenie, przekazanie do krajów trzecich.

działań audytowych. Jeżeli audyt jest przeprowadzany przez kilku audytorów, plan audytu musi zawierać jasny opis ich zadań, tak aby każdy audytor dokładnie znał swoje obowiązki. Plan audytu musi zawierać co najmniej następujące elementy:

- Zlecenie inspekcji: zakres audytu, zespół audytorów, terminy audytu, inne ważne aspekty dotyczące audytu.
- Przygotowanie inspekcji: lista aspektów do audytu, zorganizowanie zespołu/kto jest za co odpowiedzialny.
- Listy kontrolne i/lub kwestionariusze oraz inne przydatne informacje (teksty aktów prawnych, dokumenty dotyczące środowiska pracy, etc.).
- Zadbanie o bezpieczne przechowywanie dowodów (ze względu na możliwy wrażliwy charakter danych związanych z egzekwowaniem prawa należy się upewnić, czy dowody będą przekazywane do organu ochrony danych lub czy będą zastosowane inne środki).
- Musi być dostępna struktura sprawozdawczości z audytu, ustalająca, w jaki sposób wyniki audytu będą dokumentowane i przedstawiane.
- Harmonogram audytu.
- Struktura przedstawiania sprawozdań z wyników.

Przeprowadzenie audytu / sprawozdanie z audytu

- Podczas inspekcji wszyscy audytorzy muszą zgromadzić wystarczającą ilość dowodów na poparcie swoich ustaleń i wniosków, aby przedstawić dobrze uzasadnione sprawozdanie z inspekcji. Na dowody składają się dwa komponenty: sprawozdania z wywiadów oraz pisemne oświadczenia audytora dotyczące ustaleń, spostrzeżeń i decyzji, które są istotne dla sprawozdania z inspekcji oraz, gdy to konieczne, potwierdzenie tych ustaleń (wydruk systemu lub inne dokumenty).
- Audytor (audytorzy) musi (muszą) zawsze pracować zgodnie ze zleceniem.

Sprawozdanie z audytu

Ostatnim krokiem inspekcji jest przedstawienie ustaleń w sprawozdaniu, wraz z oceną oraz (gdy to konieczne) zaleceniami. Sprawozdanie zawiera całkowitą oceną przedmiotów audytu w oparciu o wymogi w zakresie ochrony danych.

Mimo że zależy to od profesjonalnego osądu audytora, może on wziąć pod uwagę następujące kwestie: (1) wrażliwość danych osobowych, które są przetwarzane, (2) liczbę osób, na które ma to wpływ, (3) czy działalność lub praktyka jest sprzeczna z zasadami struktury prawnej

lub w inny sposób niezgodna z prawem, (4) charakter i częstotliwość występowania takich działań lub praktyk.

Sprawozdanie z audytu powinno obejmować co najmniej:

- ❖ - Streszczenie.
- ❖ - Spis treści
- ❖ - Zleceniodawca i audytor (w tym podpis audytora)
- ❖ - Szczegółowe sprawozdanie
 - Cel audytu
 - Zakres audytu, to jest:
 - Przedmiot
 - Aspekt(y): poufność, integralność, ciągłość oraz możliwość audytu
 - Wymogi (wynikające z ustawodawstwa krajowego i europejskiego)
 - Metodologia audytu, podejście i dogłębność
 - Data
 - Wszelkie ograniczenia zastosowane względem audytu
 - Opinia
 - Szczegółowe ustalenia, oceny i zalecenia
 - Wybrany rozdział, w którym audytowany (audytowani) / zleceniodawca może przedstawić oficjalną odpowiedź (odpowiedzi)

Sprawozdanie może zawierać zalecenia. Odpowiedzialność za realizację zalecanych rozwiązań oraz za nadzorowanie postępu w dokonywaniu ustaleń z audytu ponosi kierownictwo. Zaleca się, aby audytor zaproponował w sprawozdaniu ramy czasowe na dalsze działania.

Audyt adekwatności

Podczas audytu adekwatności audytor powinien poddać przeglądowi i ocenie całą istotną dokumentację dotyczącą ochrony danych przechowywaną przez organizację wymiaru sprawiedliwości. Zazwyczaj obejmuje ona polityki ochrony prywatności i bezpieczeństwa oraz wszystkie istotne procedury pisemne. Produktem końcowym będzie sprawozdanie z audytu adekwatności.

Na audyt adekwatności składają się następujące kroki:

- Audytor zobowiązany jest do przestudiowania wszystkich instrumentów prawnych dotyczących ochrony danych i zbiorów policyjnych, etc.

- Audytor prosi organ wymiaru sprawiedliwości o przesłanie wszystkich istotnych dokumentów do celów oceny.
- Audytor analizuje, czy dostępna dokumentacja (polityki, procedury, etc.) jest wystarczająca i adekwatna do istniejących ram prawnych. Audytor dokonuje powtórnego badania.
- Audytor dokonuje ostatecznej oceny i odsyła ją do audytowanego.

Ostateczna ocena w ramach audytu adekwatności może mieć następujące wyniki:

i. Zadowalający wynik audytu adekwatności

Jeżeli audyt adekwatności wskazuje, że organizacja wymiaru sprawiedliwości posiada udokumentowany system ochrony danych, z być może tylko niewielką liczbą luk lub braków, audytor może przejść do audytu zgodności.

ii. Niezadowalający wynik audytu adekwatności

Audyty adekwatności może wykazać, że organizacja wymiaru sprawiedliwości posiada bardzo małą ilość dokumentacji dotyczącej ochrony danych, z nieadekwatnymi procedurami i znacznymi lukami w obszarach, takich jak szkolenie uświadamiające o ochronie danych. Jeżeli audytor wykryje takie znaczące braki na tym wstępnym etapie, organ ochrony danych musi podjąć decyzję w zakresie polityki postępowania.

Audyty zgodności

Audyty zgodności jest bardzo ważny i musi być przeprowadzony na miejscu. Jego celem jest sprawdzenie, czy organizacja wymiaru sprawiedliwości działa zgodnie z udokumentowanymi politykami, kodeksami postępowania, wytycznymi i procedurami. Produktem końcowym będzie sprawozdanie z audytu zgodności.

Audyty zgodności obejmuje następujące kroki:

- Audytor zobowiązany jest do przestudiowania całej dokumentacji dotyczącej ochrony prywatności i bezpieczeństwa będącej w posiadaniu organizacji wymiaru sprawiedliwości.
- Audytor zobowiązany jest do sprawdzenia na miejscu wdrożenia wszystkich istotnych dokumentów. W trakcie tego procesu audytor musi sformułować dokładne zapytania audytowi w celu monitorowania zgodności ze wszystkimi politykami z zakresu ochrony prywatności i bezpieczeństwa.
- Audytor dokonuje ostatecznej oceny i odsyła ją do audytowanego.

Audytor ma do wyboru dwa rodzaje audytu zgodności: wertykalny i horyzontalny.

Audyt wertykalny

Wybierając ten rodzaj audytu, audytor sprawdza wszystkie aspekty systemu ochrony danych w ramach danego obszaru, funkcji lub departamentu w organizacji wymiaru sprawiedliwości. Ten rodzaj audytu koncentruje się na procesach, procedurach i rejestrach ograniczonych do samego departamentu, nie przekraczając granic międzydepartamentowych. Zaleca się, aby audytor podczas audytu zadawał także pytania personelowi, ponieważ pracownicy powinni najlepiej wiedzieć, w jaki sposób systemy departamentowe wdrażają ogólne polityki ochrony danych organizacji wymiaru sprawiedliwości.

Audyt horyzontalny

Ten rodzaj audytu obejmuje śledzenie określonego procesu w organizacji wymiaru sprawiedliwości od początku do końca. Audyt bada szereg obszarów wzajemnego oddziaływania między obszarami, funkcjami lub departamentami; ogólnie jest to klucz do zrozumienia tego, w jaki sposób organizacja wymiaru sprawiedliwości funkcjonuje i jest najlepiej przeprowadzany z doświadczonymi pracownikami operacyjnymi. Audyt horyzontalny jest zalecany, gdy procesy zachodzą na szeregu granic międzydepartamentowych.

Audyt na poziomie danych

Celem audytu na poziomie danych jest ocena, czy organ wymiaru sprawiedliwości jest uprawniony do przetwarzania określonego zestawu danych osobowych, oraz jakości takich danych.

Organ ochrony danych może podjąć decyzję o zastosowaniu takiego audytu, gdy osoba, której dane dotyczą, zwróci się z wnioskiem o zbadanie przetwarzania określonych dotyczących jej danych osobowych lub w przypadku, gdy audyt taki jest konieczny w związku z wnioskiem osoby, której dane dotyczą, o dostęp lub poprawienie danych. Jednakże taki audyt może również mieć miejsce zgodnie z polityką audytowi organu ochrony danych lub na wniosek innego organu w innym państwie UE lub na wniosek jednego ze Wspólnych Organów Nadzorczych.

Pierwszym krokiem jest zdefiniowanie celu. W zależności od powodu przeprowadzenia audytu, może być to jeden wydział w organizacji wymiaru sprawiedliwości lub cała organizacja albo nawet szereg organizacji.

Drugi krok to określenie zakresu audytu: czy będzie to ocena procesu biznesowego w jednej sprawie (czy zbiorze ad hoc) czy też ocena zawartości zbiorów stałych. W obu przypadkach

audyt może także obejmować audyt zgodności i adekwatności, jeśli konieczne ograniczony do danego zakresu. Jeżeli przedmiot audytu ma być ograniczony do jednego wydarzenia dotyczącego określonych danych, wówczas audyt na poziomie danych musi obejmować wszystkie istotne zobowiązania prawne.

Droga naprzód

Tak jak określono wcześniej w tym rozdziale na temat polityki nadzoru, wspólne podejście bazuje na określeniu wspólnych celów i używaniu tych samych metod. To całkiem nowy obszar i musi się rozwinąć w praktyce. Pozytywne doświadczenia związane z działalnością wspólnych zespołów inspekcyjnych, w których udział brali przedstawiciele wielu organów ochrony danych, co pokazuje, że możliwy jest skuteczny nadzór. Wykorzystanie przez te organy odpowiednich metod audytu okazało się być sukcesem.

Droga naprzód ma polegać na wprowadzeniu procedury, która zapewni powstanie list kontrolnych dostosowanych do wybranych celów określonych we wspólnej polityce nadzoru oraz rozwiniętych przez organy ochrony danych w celu prawdziwego sprawdzenia tych celów. WPPJ powinna wspierać takie działania.

Ocena rezultatów inspekcji będzie również zawierać ocenę wybranej metody i użytej listy kontrolnej. Wyniki tej oceny doprowadzą ostatecznie do włączenia list kontrolnych do aneksów tego katalogu dla używania w przyszłości. W kolejnych latach katalog ten będzie zawierał szeroki przegląd instrumentów możliwych do sprawowania nadzoru zarówno na podstawie wspólnej polityki jak i przepisów krajowych.

V. Wspólne działania i prawa osób, których dane dotyczą

Rozwijająca się wymiana danych między organami wymiaru sprawiedliwości w UE spowodowała sytuację, w której dane dotyczące jednej osoby mogą być przetwarzane przez różne państwa członkowskie i/lub organizacje europejskie co powoduje, że osoba taka nie może korzystać z pełni swoich praw. Różnorodność przepisów i procedur w krajach członkowskich jak również istniejące bariery językowe powoduje kolejne trudności dla osób, których dane dotyczą.

Mając na uwadze istotność zapobiegania powstawaniu przeszkód dla osób, których dane dotyczą w korzystaniu z ich praw należy rozważyć stworzenie wspólnej, efektywnej i wiarygodnej „infrastruktury” pozwalającej osobom fizycznym na wykonywanie ich praw i otrzymywanie pomocy w państwach członkowskich.

W wielu przypadkach europejskie organy ochrony danych podkreślały, że prawa osób, których dane dotyczą powinny być wykonywane w sposób zharmonizowany niezależnie od państwa członkowskiego, w którym prawa te są wykonywane i z poszanowaniem systemów i tradycji prawnych.

Informacje zebrane za pośrednictwem kwestionariusza dotyczącego praw osób, których dane dotyczą w 2006 roku pozwoliły na porównanie różnych podejść praktycznych i systemów prawnych państw członkowskich. Uzyskane odpowiedzi wskazują, że w identycznych sprawach dotyczących wykonywania praw osób, których dane dotyczą, państwa członkowskie mogą podejmować bardzo różne decyzje.

W momencie wprowadzenia zasady dostępności stymulującej wymianę danych pomiędzy państwami członkowskimi dla celów wymiaru sprawiedliwości można się jedynie zastanawiać nad możliwym wpływem tej sytuacji na osoby, których dane dotyczą i ich prawa.

Czy można oczekiwać, że osoba, której dane dotyczą zdaje sobie sprawę lub może sobie zdawać sprawę z faktu, że jej dane są przetwarzane oraz z tego że i gdzie dane te są przesyłane? Europejskie organy ochrony danych osobowych stwierdziły, że *”inicjatywy mające na celu ułatwienie stosowania przepisów prawa na terenie UE, takie jak zasada dostępności powinny być wprowadzane jedynie na podstawie odpowiednio zaplanowanych działań w zakresie ochrony danych tak, aby zapewnić wysokie standardy ochrony”*. Biorąc pod uwagę brzmienie przepisów w UE mamy do czynienia z podejściem praktycznym.

W konsekwencji mamy sytuację, w której osoba, której dane dotyczą nie jest w stanie się domyśleć ani zgadnąć w jaki sposób jej dane są przetwarzane, co powoduje, że należy znaleźć sposób wsparcia takiej osoby oraz sposób zapobiegania sytuacji, w której zasada dostępności uniemożliwia osobie korzystanie z jej praw. Dostępność do danych dla celów wymiaru sprawiedliwości powinna być wsparta zasadą dostępności do środków ochrony. W tym samym sensie tworzenie infrastruktury koniecznej do udostępniania danych powinno być wsparte tworzeniem infrastruktury służącej do efektywnej ochrony praw fundamentalnych osoby.

Pomimo wszystko dalsza harmonizacja będzie bez wątpienia ważnym krokiem do rozwiązania tego problemu, wspieranie współpracy pomiędzy organami ochrony danych będzie miała decydujące znaczenie dla wzmocnienia pozycji osoby, której dane dotyczą.

Takie działania nie są niczym nowym. Przykłady współpracy organów ochrony danych w obszarze ochrony praw osoby, której dane dotyczą mogą zostać odnalezione w Konwencji Schengen. Osoba, której dane dotyczą ma prawo zażądać dostępu do danych w każdym kraju należącym do Schengen również w przypadku kiedy dane państwo nie jest odpowiedzialne za wprowadzenie danych do Systemu Informacyjnego Schengen (SIS). Dokładne zasady dotyczące obowiązującego porządku prawnego i współpracy organów ochrony danych zostały jednoznacznie określone. Robiąc tak państwa należące do Schengen udowodniły, że ufają pomysłowi prowadzenia dalszej zharmonizowanej implementacji zasad ochrony danych. Pomimo faktu, że termin „bliska koordynacja” nie został zdefiniowany w Konwencji Schengen organy ochrony danych mają obowiązek współpracować w taki sposób aby w pełni wspierać wszystkie strony oraz osobę wykonującą swoje prawa.

Co to oznacza w praktyce? Oznacza to, że wykonywanie praw osób, których dane dotyczą powinno zostać zagwarantowane jako dostęp do sprawiedliwości co jest częścią efektywnego systemu ochrony prawnej.

Najważniejszą cechą Konwencji jest stwierdzenie, że osoba, której dane dotyczą nie zawsze będzie miała możliwość do dostania się do innego kraju lub zwrócenia się do odpowiedniego organu w innym kraju w celu powoływania się na swoje prawa np. ze względu na koszty podróży bądź barierę językową. W tym znaczeniu doświadczenia z systemem SIS i prawami osoby, której dane dotyczą dostarczają nam informacji w jaki sposób dalsza współpraca powinna się rozwijać.

Innym ważnym aspektem, który powinien być wzięty pod uwagę jest ograniczenie praw osoby, której dane dotyczą wynikające z przepisów krajowych. Prawo dostępu do danych nie jest niepodważalne i państwa członkowskie mogą przewidzieć ograniczenia tego prawa zgodnie z warunkami określonymi w Europejskiej Konwencji Ochrony Praw Człowieka i Podstawowych Wolności oraz innych międzynarodowych instrumentów. Jednakże określenie zakresu ograniczenia praw różni się dość znacznie w różnych krajach. Ponadto, jedna ze spraw pokazała, że wyniki postępowań sądowych w sprawach dotyczących skarg Schengen mogą się bardzo od siebie różnić, w zależności od kraju, w którym wniesiono odwołanie.

Zgodnie z praktyką Trybunału Sprawiedliwości, zasada pewności prawa wymaga, aby przepisy oraz praktyka były jasne i jednoznaczne dla osób fizycznych. Czy jednak osoby takie będą nadal w stanie przewidzieć praktyczne konsekwencje i być pewnymi swoich praw?

Tak jak wcześniej stwierdzono koncepcja wsparcia osób, których dane dotyczą przez organy ochrony danych nie jest niczym nowym. Konieczność współpracy organów specjalizujących się w sprawach ochrony danych została już potwierdzona w Konwencji 108. Nie bezpośrednio, ale określono obowiązek utworzenia organów ochrony danych, a pierwszy model takiej współpracy określono w art. 13 i 14 Konwencji 108. Przepisy te przewidują utworzenie ram współpracy i pomocy dla osoby rezydującej za granicą w celu umożliwienia jej wykonywania praw nie tylko w kraju, w którym dane są przetwarzane oraz za pośrednictwem organów ochrony danych.

Art. 1.5 Protokołu Dodatkowego do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych wprowadza obowiązek współpracy między organami ochrony danych państw członkowskich.

Współpraca

W oparciu o opisane doświadczenia oraz konieczność odkrycia możliwości efektywnego korzystania z praw przez osoby, których dane dotyczą w czasach gdy ujawnianie danych osobowych wydaje się normalnością wyłania się następujący scenariusz współpracy. W tych sprawach, co do zasady, zastosowanie znajdują przepisy danego kraju.

Termin „prawa osoby, której dane dotyczą” odnosi się do prawa do bycia poinformowanym o tym czy dane są przetwarzane, przedstawione w sposób zrozumiały oraz do dokonania korekty danych niezgodnych z rzeczywistością.

1. Przepisy prawa krajowego kraju, w którym dane są wykonywane stosowane są zgodnie ze sposobem postępowania stosowanym przez organy wymiaru sprawiedliwości.

To sytuacja istniejąca i raczej nie ulegnie zmianie zbyt szybko. Należy wspomnieć, że przedmiot prośby osoby, której dane dotyczą może być przekazany przez organy innego kraju europejskiego lub organizacji takich jak Europol czy Eurojust.

W przypadku zaangażowania krajowych organów ochrony danych w ocenę każdej prośby i danych z innego kraju bądź organizacji to taki organ może potrzebować opinii od organu bądź

organizacji, która przesłała dane. Mamy z tym z pewnością do czynienia gdy prośba odnosi się korekty lub usunięcia danych. Taka współpraca jest konieczna nie tylko przy rozpatrywaniu prośb; jeśli wygląda na to, że dane powinny być poprawione czy usunięte to organy ochrony danych powinny upewnić się czy dane zostaną usunięte po obu stronach. Taka współpraca odbywa się we wspólnych organach nadzorczych.

2. Kiedy osoba, której dane dotyczą ma zamiar korzystać ze swoich praw w innym kraju europejskim lub w kraju, w którym mieszka oraz gdy podejrzewa, że jego dane są przetwarzane to podstawową zasadą jest, że prośba powinna zostać przesłana bądź kompetentnego organu w państwie członkowskim lub do organu ochrony danych w tym kraju. Jednakże, często osoba nie jest w stanie rozstrzygnąć do jakiego organu powinna się zwrócić zwłaszcza, gdy mamy do czynienia z organami wymiaru sprawiedliwości. Aby zapobiec sytuacji, w której osoba nie będzie mogła korzystać ze swoich praw konieczna jest możliwość zwrócenia się o pomoc do krajowego organu ochrony danych. Organ ten we współpracy z innymi ma obowiązek poinformować osobę do kogo powinna się zwrócić.

Jednakże, mając na uwadze wpływ ujawniania danych oraz konsekwencje tego, że dane dotyczące jednej osoby mogą być przetwarzane przez wiele europejskich krajów oraz międzynarodowych organizacji to prawdopodobnie konieczne będzie nawiązanie innej, szerszej współpracy.

3. Jeśli osoba, której dane dotyczą wykonuje dostęp do danych w kraju, w którym mieszka i jeśli istnieje jasny dowód na to, że jego dane przekazywane są do innych krajów europejskich lub organizacji to obecna procedura wymaga aby zwrócił się do organizacji bądź kraju co do którego jest podejrzenie, że właśnie do niego dane zostały przesłane. To bardzo nieefektywna praktyka i osoba, której dane dotyczą powinna mieć możliwość skutecznego korzystania ze swoich praw. Osoba taka może zwrócić się do krajowego organu ochrony danych w kraju, w którym prawo dostępu jest wykonywane. Pomoc taka może polegać na sprawdzeniu czy dane naprawdę są przetwarzane przez inne kraje i organizacje europejskie. W przypadkach, w których prawo ograniczenia dostępu będzie miało zastosowanie w szczególnej sprawie takiej jak dochodzenie może mieć miejsce z urzędu.

W przypadkach gdy dochodzenie udowodni, że dane są rzeczywiście przekazywane do innego kraju bądź organizacji to organ ochrony danych powinny wystąpić do organów tych

krajów z prośbą o rozpoczęcie procedury dostępu. Organy krajowe powinny potraktować taką prośbę jako prośbę skierowaną na podstawie przepisów prawa krajowego i złożyć raport organowi wysyłającemu prośbę.

Osoba, której dane dotyczą będzie poinformowana o wynikach.

4. Jeśli w rezultacie wykonywania prawa dostępu dane zostaną ujawnione w sposób nieprawidłowy bądź niezgodnie z prawem a zostały one przekazane innym organom to wymagana jest aktywność organu ochrony danych. Na wniosek osoby bądź z urzędu organ ochrony danych powinien skontaktować się z organem, do którego przekazano dane. Organ, który został poproszony o współpracę powinien potraktować taką prośbę zgodnie ze wszystkimi wymogami swojego prawa krajowego. Jego decyzje i ustalenia muszą zostać przekazane organowi występującemu z prośbą.

Osoba powinna zostać poinformowana o wynikach dochodzenia zgodnie z przepisami kraju, w którym wykonywane było prawo dostępu. Organ informujący osobę powinien wziąć pod uwagę sugestie i ustalenia organów współpracujących.

5. Jeśli procedura podjęta w państwie europejskim kończy się wydaniem decyzji przez sąd, a decyzja ta zawiera zobowiązanie do poprawy bądź usunięcia danych przekazanych przez inny kraj bądź organizację to istnieje konieczność poinformowania tego kraju o wydaniu takiej decyzji. Pomimo faktu, że nie istnieje instrument prawny regulujący dwustronne uznawanie takich decyzji (oprócz przepisów art. 111 Konwencji Schengen oraz art. 24(7) Konwencji o Europolu), obowiązek zapewnienia przetwarzania odpowiednich danych (art. 5(d) Konwencji 108 oraz zasada 3.1 Rekomendacji R87(15)) zmusza kraje do przynajmniej sprawdzenia potrzeby dokonania korekty lub usunięcia danych. Należy poinformować zarówno organ przekazujący dane jak i organ nadzorujący o tym, że nakaz dokonania korekty bądź usunięcia wynika z decyzji sądu. Pomimo, że samo wydanie takiej decyzji przez sąd nie jest równoznaczne z tym, że organ przekazujący musi dane poprawić lub usunąć to jednak ważne jest spełnienie obowiązku informacyjnego wobec wszystkich organów. Taką informację zobowiązany jest przekazać organ ochrony danych jeśli jest zaznajomiony z taką sprawą. Również jeśli to organ ochrony danych dowie się o takiej decyzji powinien poinformować organizację wysyłającą o tym czy decyzja nakazuje np. poprawę bądź usunięcie danych.

Praktyka współpracy

Język

Obecna praktyka pokazuje, że zapytania i odpowiedzi udzielane są w językach narodowych. Czasami organy zobowiązane są do prowadzenia korespondencji w języku urzędowym. Może jednak dojść do sytuacji, w której osoba otrzyma informację w niezrozumiałym dla niej języku.

Dopuszczalne są trzy scenariusze:

- cała korespondencja w jednym języku, sugerowany angielski.
- cała korespondencja w językach stron i to one odpowiadają za ewentualne tłumaczenia.
- organy ochrony danych porozumiewają się co do języka, w którym prowadzona jest korespondencja.

Ograniczenia czasowe

Prośby powinny być rozpatrywane bez zbędnej zwłoki.

Osoba kontaktowa

Dla ułatwienia dalszej współpracy w załączniku 5 znajdzie się lista osób kontaktowych.

Formularze

Opracowano formularze do użytku przez organy ochrony danych.

Ewaluacja

Współpraca pomiędzy organami ochrony danych tak jak opisano ją w tym rozdziale jest rzeczą nową. Istnieje konieczność czasowej oceny jej skuteczności i tego czy nie powinna zostać poszerzona. Mając to na uwadze WPPJ dokona oceny współpracy dotyczącej praw osoby, której dane dotyczą co dwa lata.

Załączniki:

- 1. Audyt adekwatności przepisów** (brak dokumentu)
- 2. Audyt zgodności** (brak dokumentu)
- 3. Audyt poziomu ochrony danych** (brak dokumentu)
- 4. Raport z audytu** (brak dokumentu)
- 5. Współpraca i prawa osób, których dane dotyczą** (lista kontaktów, dokument pusty)

Formularz

Prośba o nawiązanie współpracy w języku angielskim.

ZAŁĄCZNIK 6 Lista kontrolna oceniająca środki wdrażające koncepcję dostępności w obszarze egzekwowania prawa

(Przyjęty podczas Wiosennej Konferencji Europejskich Organów Ochrony Danych, Cypr, 10-11 maja 2007 r.)

I. Prawo i ocena

Każdy środek musi przewidziany prawem.

Prawo musi być zgodne z rygorystycznymi kryteriami takimi, jak precyzyjność oraz pewność i przewidywalność.

Ponadto ustawodawstwo zawsze musi:

- Określać przyczyny
- Cel oraz
- Warunki przetwarzania
- Wprowadzać adekwatny i skuteczny system niezależnego nadzoru.

II. Niezbędność i proporcjonalność

Środek powinien stanowić niezbędne zabezpieczenie.

A. Ocena już istniejących środków prawnych zezwalających na przetwarzanie, w tym wymianę danych.

❖ Czy środki te nie są wystarczające?

- Gdy środek prawny jest wykorzystywany skutecznie, ale ewidentnie nie zapewnia wystarczającego i skutecznego elementu w walce z przestępczością, może to być wskazówką, że potrzebny jest inny środek.

❖ Czy wdrożenie środka i dalsze działania są nieskuteczne?

- Gdy ocena wykazuje, że już istniejące możliwości nie są wykorzystywane wystarczająco, może stworzyć to znaczne wątpliwości co do tego, czy proponowany nowy środek będzie uzasadnionym wyjątkiem od zasady ograniczenia celu.

❖ W przypadku, gdy ocena ta wskazuje, że środek prawny mógłby być uzasadniony, powinny być spełnione następujące warunki proporcjonalności:

B. Proporcjonalność

❖ Środek powinien być zaprojektowany tak, aby osiągnąć

- Skuteczne egzekwowanie,
- Minimalną ingerencję w prywatność.

❖ Oznacza to test proporcjonalności obejmujący następujące elementy:

- Środek musi być odpowiedni, co oznacza, że jego przyczynienie się do egzekwowania prawa musi być wyraźnie pokazane.
- Środek nie może być nadmierny, co oznacza, że środek o mniejszym wpływie nie może przynieść takiego samego wyniku.
- Musi istnieć równowaga: gdy wpływ na ochronę danych może być uzasadniony w celu zwalczania terroryzmu lub innych poważnych przestępstw (zgodnie z artykułem 2(2) Decyzji ramowej w sprawie europejskiego nakazu aresztowania), nie oznacza to, że dane te mogą być udostępniane w celu zwalczania niewielkich wykroczeń.

❖ Instrument prawny powinien podlegać obowiązkowej ocenie.

III. Określone warunki

Chodzi o różne rodzaje danych: począwszy od danych identyfikacyjnych (wykorzystywanych zarówno do identyfikacji osoby, której dane dotyczą, jak i do kontaktowania się z nią) oraz ogólne i szczegółowe dane opisowe (np. inteligencja), po rodzaje danych określanych na podstawie biometrii (np. odciski palców lub cyfrowy zapis DNA) oraz dane szczególnie chronione (zgodnie z artykułem 8 dyrektywy 95/46). Podobnie zaangażowane są różne rodzaje osób, których dane dotyczą: podejrzani, niepodejrzani, świadkowie, osoby skazane lub uniewinnione. Należy wziąć pod uwagę następujące punkty:

A. Ustawodawstwo musi:

- wprowadzić rozróżnienie między tymi danymi,
- przewidzieć konkretne dodatkowe zabezpieczenia w odniesieniu do przetwarzania danych, które mogą stwarzać konkretne zagrożenia dla praw i wolności osób, których dane dotyczą, w szczególności wykorzystywanie danych szczególnie chronionych przez wprowadzenie ruchomej skali środków ochronnych, gdzie charakterystyka danych decyduje o szczególnych warunkach i ograniczeniach ich wykorzystania.
- obejmować kryteria umożliwiające jasne rozróżnienie między danymi osobowymi, rozróżniając kategorie danych osobowych i ich dostępność dla konkretnych kategorii przestępstw. (Na przykład osoby uwolnione od zarzutów lub osoby, przeciwko którym nie wysunięto zarzutów, powinno się wyraźnie odróżnić od osób skazanych. Dane dotyczące niepodejrzanych i świadków powinno się wyraźnie odróżnić od danych dotyczących podejrzanych).

B. Należy wprowadzić określone środki mające na celu ocenę jakości danych, aby zagwarantować możliwie najwyższy poziom jakości danych, zanim dane zostaną udostępnione. Z uwagi na wpływ wykorzystania danych do celów egzekwowania prawa,

muszą istnieć wystarczające środki techniczne i organizacyjne w celu zagwarantowania jakości danych. W takim przypadku nie można przewidzieć gwarancji, należy to wskazać, a wykorzystanie tych danych musi być ograniczone do konkretnego działania z zakresu egzekwowania prawa, z dodatkowymi zabezpieczeniami. Musi istnieć obowiązek informowania odbiorcy danych osobowych o wszelkich zmianach tych danych.

C. Wykorzystanie danych biometrycznych w obszarze egzekwowania prawa wymaga dodatkowych zabezpieczeń. W szczególności wykorzystaniu tych danych do identyfikacji osób, czasami przy wykorzystaniu systemów, które przetwarzają ogromne ilości tych danych, muszą towarzyszyć procedury umożliwiające osobie uzyskanie ponownego sprawdzenie wyniku porównania.

D. Określone operacje przetwarzania, które mogą stwarzać konkretne zagrożenia (np. przeszukiwanie dużych ilości danych, konkretne techniki nadzoru), wymagają dodatkowych zabezpieczeń dla wykorzystania tych danych oraz monitorowania tych operacji.

E. Istotne będzie zapewnienie, za pomocą środków technicznych i organizacyjnych oraz procedur, że odbiorcy danych osobowych otrzymują niezbędne informacje do wykorzystania danych do celów, dla których zostały przekazane, oraz w celu ich aktualizacji.

F. Gdy inicjatywa lub propozycja daje do wyboru przetwarzanie danych osobowych na poziomie centralnym lub ich przetwarzanie zdecentralizowane, wybór ten musi być umotywowany nie tylko operacyjnością. Wybór taki musi także uwzględniać potrzebę zagwarantowania możliwie najwyższego poziomu jakości danych oraz standardów ochrony danych. Gdy przetwarzanie zdecentralizowane przewiduje lepsze zabezpieczenia, przetwarzanie scentralizowane nie powinno stanowić jednej z możliwości.

IV. Dostęp organów wymiaru sprawiedliwości do danych osobowych

- Rutynowy dostęp do danych osobowych powinien być zakazany.
- Dostęp musi być ograniczony do konkretnych przypadków lub do konkretnego zadania z zakresu egzekwowania prawa.
- Kontrola wykorzystania tego dostępu musi być wystarczająco zabezpieczona.
- Gdy proponowany jest bezpośredni dostęp do danych, wymagane jest wykorzystanie systemów indeksowych (tzw. systemów hit-no-hit) oraz wystarczające kontrole dostępu.
- Organy odbierające muszą być wyraźnie określone.

V. Kontrola i nadzór

- Poza standardowymi kompetencjami organów egzekwowania prawa, organów sądowych oraz organów ochrony danych ds. kontrolowania i nadzorowania przetwarzania danych, działaniom, które mogą stwarzać konkretne zagrożenia dla praw i wolności osoby, której dane dotyczą, powinny towarzyszyć dodatkowe dostosowane środki kontroli i nadzoru wszystkich działań operacyjnych w tym wykorzystania i niewłaściwego wykorzystania danych osobowych.
- Potrzebne są szczegółowe przepisy zapobiegające wystąpieniu trudności wynikających z wymiany danych między państwami członkowskimi. Jako że dane te są dostępne w kilku jurysdykcjach, należy zapewnić, że kontrola i nadzór będą skuteczne we wszystkich zaangażowanych jurysdykcjach.