REKOMENDACJA R(87)15

KOMITETU MINISTRÓW RADY EUROPY

O OCHRONIE DANYCH OSOBOWYCH WYKORZYSTYWANYCH W SEKTORZE POLICJI[1]

z 17 września 1987 roku

Komitet Ministrów,
na podstawie artykułu 15.b. Statutu Rady Europy,

Zważywszy, że celem Rady Europy jest urzeczywistnienie jak najściślejszego związku pomiędzy jej Państwami Członkowskimi;

Świadom wzrastającego wykorzystywania w sektorze Policji danych osobowych stanowiących przedmiot automatycznego przetwarzania, jak też korzyści, jakie wynikają z wykorzystania komputerów oraz innych środków technicznych w tej dziedzinie;

Zważywszy, z drugiej strony, na niepokój, jaki rodzi możliwe ryzyko nadużycia technik automatycznego przetwarzania dla życia prywatnego jednostek;

Uznając konieczność pogodzenia, z jednej strony, zainteresowania społeczeństwa zapobieganiem i zwalczaniem przestępczości oraz utrzymaniem porządku publicznego, a z drugiej strony, interesów jednostki oraz jej prawa do poszanowania prywatności;

Uwzględniając postanowienia Konwencji o ochronie osób w zakresie zautomatyzowanego przetwarzania danych osobowych z dnia 28 stycznia 1981 roku, a w szczególności odstępstwa dozwolone na podstawie Artykułu 9;

Kierując się duchem postanowień artykułu 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności;

Zaleca Rządom Państw Członkowskich:
- inspirowanie się w ich prawie i w praktyce krajowej Zasadami dołączonymi do niniejszej Rekomendacji; oraz

- upowszechnianie postanowień załączonych do niniejszej Rekomendacji, a w szczególności informowanie o prawach, jakie ich wprowadzenie zapewnia jednostce.

---

[1] Przy przyjmowaniu niniejszej Rekomendacji:

- na mocy z art. 10.2.c Regulaminu wewnętrznego spotkań delegatów Ministrów, delegat Irlandii zastrzegł prawo swojego rządu do dostosowania się lub nie do niniejszej Rekomendacji, delegat Zjednoczonego Królestwa zastrzegł prawo swojego rządu do podporządkowania się lub nie do zasad 2.2 i 2.4 Rekomendacji, a delegat Federalnej Republiki Niemiec zastrzegł prawo swojego rządu przyjęcia lub nie zasady 2.1 Rekomendacji;
- na mocy art. 10.2.d wyżej wymienionego Regulaminu wewnętrznego, delegat Szwajcarii wstrzymał się zaznaczając, że zastrzega prawo swojego rządu do przyjęcia bądź nie niniejszej Rekomendacji oraz, że jego wstrzymanie się nie powinno być rozumiane jako wyraz dezaprobaty w całości.
- Pismem z dnia 10 grudnia 1997 roku, Rząd Irlandii zawiadomił Sekretariat o rezygnacji z zastrzeżeń odnośnie punktów: 2.2, 2.3, 2.4. zgłoszonych w czasie przyjmowania Rekomendacji.

ZAŁĄCZNIK DO REKOMENDACJI

Zakres stosowania i definicje

Zasady ogłoszone w niniejszej Rekomendacji mają zastosowanie do gromadzenia, rejestrowania, wykorzystywania i przekazywania dla potrzeb Policji danych osobowych, które podlegają automatycznemu przetwarzaniu.

Dla celów niniejszej Rekomendacji, wyrażenie „dane osobowe" obejmuje wszelkie informacje dotyczące osoby fizycznej zidentyfikowanej bądź możliwej do zidentyfikowania. Osoby fizycznej nie uważa się za „dającą się zidentyfikować", jeśli tego rodzaju identyfikacja wymaga nadmiernego zaangażowania czasu, sił i środków.

Wyrażenie „dla potrzeb Policji" obejmuje całość zadań spoczywających na władzach policyjnych, które służą zapobieganiu i zwalczaniu przestępstw oraz utrzymaniu porządku publicznego.

Wyrażenie „organ odpowiedzialny" (*administrator zbioru)* oznacza organ, służbę bądź jakąkolwiek inną instytucję publiczną, która posiada kompetencje - zgodnie z prawem krajowym — w zakresie decydowania o przeznaczeniu zautomatyzowanego zbioru, kategorii danych osobowych, które mają podlegać rejestrowaniu, jak również o działaniach, jakim dane te będą poddane.

Państwo Członkowskie może rozszerzać Zasady zawarte w niniejszej Rekomendacji na dane osobowe niepodlegające zautomatyzowanemu przetwarzaniu.

Nie powinno się przetwarzać danych ręcznie w celu uniknięcia postanowień niniejszej Rekomendacji.

Państwo Członkowskie może rozszerzać Zasady zawarte w niniejszej Rekomendacji na dane dotyczące ugrupowań, stowarzyszeń, fundacji, spółek, korporacji bądź jakichkolwiek innych organizacji grupujących - bezpośrednio bądź pośrednio - osoby fizyczne, mające lub nie mające osobowości prawnej.

Postanowień niniejszej Rekomendacji nie należy interpretować jako ograniczających, bądź w inny sposób godzących w swobodę, jaką dysponuje Państwo Członkowskie, jeśli chodzi o rozszerzenie - zależnie od przypadku - niektórych jej Zasad na gromadzenie, rejestrowanie oraz wykorzystywanie danych osobowych dla potrzeb bezpieczeństwa Państwa.

ZASADY PODSTAWOWE

Zasada l - Kontrola i notyfikacja

1.1. Każde Państwo Członkowskie powinno dysponować niezależnym i zewnętrznym w stosunku do Policji organem nadzorczym, upoważnionym do czuwania nad przestrzeganiem Zasad zawartych w niniejszej Rekomendacji.

1.2. Wprowadzanie nowych środków technicznych służących przetwarzaniu danych może mieć miejsce tylko wtedy, gdy zostaną powzięte wszelkie możliwe środki zabezpieczające, by ich wykorzystywanie pozostawało w zgodzie z literą prawa obowiązującego w dziedzinie przetwarzania danych.

1.3. Administrator danych powinien konsultować się z organem nadzorczym zawczasu i każdorazowo, gdy wprowadzenie technik automatycznego przetwarzania rodzi pytania dotyczące stosowania niniejszej Rekomendacji.

1.4. Stałe zautomatyzowane zbiory winny być zgłoszone do organu nadzorczego. Zgłoszenie powinno określać charakter zgłaszanego zbioru, tożsamość administratora danych, przeznaczenie zbioru, kategorie danych, jakie ma on zawierać, jak również odbiorców, którym dane mają być udostępniane.

Zbiory tworzone *ad hoc*, przy okazji poszczególnych spraw, również winny być zgłaszane do organu nadzorczego, czy to na warunkach z nim ustalonych stosownie do specyfiki tego rodzaju danych, czy też zgodnie z ustawodawstwem krajowym.

Zasada 2 - Gromadzenie danych

2.1. Gromadzenie danych osobowych dla potrzeb Policji winno ograniczać się do tych danych, które są konieczne dla zapobieżenia realnemu niebezpieczeństwu, bądź zwalczeniu określonego przestępstwa.

Wszelkie wyjątki od powyższego postanowienia winny być przedmiotem szczególnego ustawodawstwa krajowego.

2.2. Tam, gdzie dane dotyczące osoby były gromadzone i przechowywane bez jej wiedzy, powinna ona - jeśli dane takie nie zostały usunięte - zostać poinformowana w miarę możliwości o tym, iż informacje o niej są przetwarzane w zbiorze. Należy tego dokonać, gdy tylko przestanie istnieć ryzyko, iż przedmiot działań Policji poniesie jakąkolwiek szkodę wynikającą z ujawnienia osobie, której dane dotyczą faktu istnienia tych informacji.

2.3. Gromadzenie danych przy wykorzystaniu technik inwigilacyjnych bądź innych środków zautomatyzowanych powinno być unormowane w przepisach szczególnych.

2.4. Gromadzenie danych o osobach fizycznych wyłącznie z tej racji, że mają one konkretne pochodzenie rasowe, określone przekonania religijne, określone zachowania seksualne, bądź takie a nie inne poglądy polityczne, albo że należą do określonych ruchów lub organizacji, które nie są prawnie zakazane, winno być zabronione. Gromadzenie tej kategorii danych jest niedopuszczalne, chyba że jest to absolutnie konieczne dla potrzeb konkretnego śledztwa.

Zasada 3 - Rejestracja danych

3.1. Na ile to tylko możliwe, rejestrowanie danych osobowych dla potrzeb Policji powinno dotyczyć jedynie konkretnych danych, niezbędnych do wypełniania zgodnych z prawem zadań realizowanych przez organy policyjne, w granicach przewidzianych przez prawo krajowe oraz postanowienia wynikające z prawa międzynarodowego.

3.2. Różne kategorie rejestrowanych danych powinny być - na ile to tylko możliwe - zróżnicowane w zależności od stopnia ich dokładności lub prawdziwości, a w szczególności dane oparte na faktach winny być odróżnione od danych opartych na osobistych poglądach lub ocenach.

3.3. W przypadku, gdy dane gromadzone dla celów administracyjnych podlegają rejestracji na stałe, powinny się one znaleźć w odrębnym zbiorze. W każdym przypadku należy powziąć środki zapewniające, by dane administracyjne nie podlegały regułom stosującym się do danych policyjnych.

Zasada 4 - Wykorzystywanie danych przez Policję

4. Z zastrzeżeniem Zasady 5, dane osobowe - gromadzone i rejestrowane przez Policję dla potrzeb realizowanych przez nią zadań - powinny służyć wyłącznie tym celom.

Zasada 5 - Przekazywanie zbiorów danych

5.1. *Przepływ danych w obrębie sektora Policji*

Przekazywanie danych pomiędzy służbami policyjnymi w celu wykorzystania ich dla potrzeb Policji winno być dozwolone jedynie w przypadku, gdy istnieje prawnie uzasadniony interes przemawiający na rzecz tego rodzaju przekazywania, odbywającego się w ramach określonych prawem zadań tych służb.

5.2.i. *Przekazywanie danych innym organom publicznym*

Przekazywanie danych organom publicznym winno być dozwolone jedynie w przypadku, gdy:

a. istnieje wyraźny obowiązek prawny bądź zezwolenie organu nadzorczego; lub

b. dane takie są odbiorcy niezbędne dla wypełnienia jego własnego zgodnego z prawem zadania oraz pod warunkiem, że cel gromadzenia lub przetwarzania dokonywanego przez takiego odbiorcę nie jest niezgodny z celem pierwotnie przewidzianym, oraz że nie stoi on w sprzeczności z prawnymi obowiązkami organu przekazującego.

5.2.ii. Ponadto, przekazywanie danych innym organom publicznym jest w wyjątkowych sytuacjach dozwolone, jeśli w konkretnym przypadku:

a. nie ma wątpliwości, iż przekazywanie danych leży w interesie osoby, której dane dotyczą lub jeśli ona sama wyrazi na to zgodę, bądź też okoliczności pozwalają na jednoznaczne domniemanie takiej zgody; lub jeśli

b. takie przekazywanie danych jest konieczne dla uniknięcia poważnego i bezpośredniego niebezpieczeństwa.

5.3.i. *Przekazywanie danych osobom prywatnym*

Przekazywanie danych osobom prywatnym winno być dozwolone jedynie w przypadku, gdy w grę wchodzi wyraźne zobowiązanie prawne lub upoważnienie, bądź też upoważnienie organu

nadzorczego.

5.3.ii. Przekazywanie danych osobom prywatnym będzie wyjątkowo dozwolone, jeśli w konkretnym przypadku:

a. nie ma wątpliwości, iż przekazywanie danych pozostaje w interesie osoby, której dane dotyczą lub jeśli ona sama na to się godzi, bądź też okoliczności pozwalają na niedwuznaczne domniemanie takiej zgody; albo jeśli

b. przekazywanie danych jest konieczne dla uniknięcia poważnego i bezpośredniego niebezpieczeństwa.

5.4. *Przekazywanie danych za granicę*

Przekazywanie danych organom zagranicznym winno się ograniczać do służb policyjnych. Winno ono być dozwolone tylko w przypadku, gdy:

a. istnieje wyraźny przepis prawny wynikający z prawa krajowego, bądź z prawa międzynarodowego;

b. w przypadku braku takiego przepisu uznanie, że przekazywanie danych jest konieczne dla zapobieżenia poważnemu i bezpośredniemu niebezpieczeństwu, albo dla ścigania z mocy prawa poważnego przestępstwa; ale pod warunkiem, że nie godzi to w unormowania krajowe dotyczące ochrony danych osoby, której te dane dotyczą.

5.5.i. *Wnioski dotyczące przekazywania danych*

Z zastrzeżeniem przepisów szczególnych ustawodawstwa krajowego bądź umów międzynarodowych, wnioski o przekazywanie danych za granicę powinny zawierać wskazania dotyczące organu lub osoby, które je składają, jak również uzasadnienie takiego wniosku i cel przekazania.

5.5.ii. *Warunki przekazywania*

O ile to tylko możliwe, jakość danych powinna podlegać weryfikacji najpóźniej przed ich przekazaniem za granicę. Podczas każdorazowego przekazywania danych, o ile to tylko możliwe, należy wskazać decyzje sądowe, w tym również decyzje w sprawie umorzenia, a dane oparte na poglądach i ocenach osobistych zweryfikować u źródła; należy określić stopień ich prawdziwości i dokładności.

Gdyby się okazało, iż dane nie są dokładne czy aktualne, nie powinno się ich przekazywać za granicę; gdyby jednak takie dane zostały przekazane, organ wysyłający powinien - w miarę możliwości - poinformować o ich wadach wszystkich odbiorców, którym dane są przekazywane.

5.5.iii. *Gwarancje dotyczące przekazywania*

Dane przekazywane innym organom publicznym, osobom prywatnym bądź organom zagranicznym nie powinny być wykorzystywane do celów innych, niż cele oznaczone we wniosku o ich

przekazanie.

Wykorzystanie danych do innych celów winno być uzależnione od zgody organu wysyłającego, bez szkody dla postanowień wynikających z punktów 5.2.-5.4. Zasady 5.

5.6. *Łączenie zbiorów i dostęp w sieci (on-line)*

Łączenie zbiorów danych policyjnych ze zbiorami używanymi do innych celów jest dopuszczalne po spełnieniu jednego z następujących warunków:

a. udzielenie zgody przez organ nadzorczy celem ścigania konkretnego przestępstwa; albo

b. zgodność z jednoznacznym przepisem prawnym.

Bezpośredni dostęp w sieci (on-line) do zbiorów winien być dozwolony jedynie w sytuacji, gdy jest to zgodne z ustawodawstwem krajowym, które powinno uwzględniać Zasady 3-6 niniejszej Rekomendacji.

Zasada 6 - Informacja publiczna o zbiorach, prawo dostępu do zbiorów policyjnych, prawo do sprostowania i prawo do odwoływania się.

6.1. Organ nadzorczy winien powziąć środki służące zapewnieniu, by opinia publiczna była poinformowana o istnieniu zbiorów policyjnych, czyniąc je przedmiotem zgłoszenia, jak również o prawach osób, których dane zawarte są w takich zbiorach. Urzeczywistnienie powyższej Zasady winno uwzględniać specyfikę zbiorów tworzonych *ad hoc*, *w* szczególności konieczność zagwarantowania, by realizacja przez Policję zgodnego z prawem zadania nie została zagrożona.

6.2. Osoba, której dane dotyczą winna dysponować możliwością uzyskania dostępu do zbiorów policyjnych w odpowiednim czasie i bez nadmiernej zwłoki, zgodnie z procedurą przewidzianą prawem krajowym.

6.3. Osoba, której dane dotyczą winna mieć możliwość sprostowania, jeżeli jest taka konieczność, dotyczących jej danych zawartych w zbiorach policyjnych.

Dane osobowe, które w rezultacie skorzystania z prawa dostępu okazały się nieścisłe, bądź które wydają się nadmierne ilościowo, niedokładne czy bez związku ze sprawą - w powołaniu się na jedną z Zasad zawartych w niniejszej Rekomendacji - powinny zostać usunięte lub skorygowane, albo stać się przedmiotem dołączonego do zbioru oświadczenia wnoszącego o sprostowanie danych.

Tego rodzaju działania, polegające na usunięciu lub sprostowaniu danych, powinny także dotyczyć - w miarę możliwości - wszystkich dokumentów dołączonych do zbiorów policyjnych, a jeśli działania takie nie zostaną podjęte natychmiast, winny być wprowadzone najpóźniej przy okazji kolejnego przetwarzania lub przekazywania danych.

6.4. Korzystanie z prawa dostępu, sprostowania lub usunięcia może podlegać ograniczeniom tylko w takim stopniu, w jakim tego rodzaju ograniczenie jest konieczne dla wypełnienia zgodnego z

prawem zadania Policji, bądź też konieczne jest dla ochrony osoby, której dane dotyczą, albo dla ochrony praw i wolności innych osób.

W interesie osoby, której dane dotyczą, w szczególnych przypadkach, prawo może wykluczyć udostępnienie danych w formie pisemnej.

6.5. Odmowa bądź ograniczenie korzystania z powyższych praw powinny być uzasadnione na piśmie. Nie można odmówić osobie, której dane dotyczą wydania uzasadnienia, chyba, że jest to niezbędne dla wypełnienia zgodnego z prawem zadania Policji, bądź konieczne dla ochrony praw i wolności innych osób.

6.6. W przypadkach, w których osobie, której dane dotyczą odmówiono dostępu do dotyczących jej danych osobowych, osoba ta winna dysponować możliwością odwołania się do organu nadzorczego lub do innego niezależnego organu, który stwierdzi, czy odmowa była odpowiednio uzasadniona.

Zasada 7 - Okres przechowywania oraz aktualizacja danych

7.1. Należy przedsięwziąć środki, by dane osobowe przechowywane dla potrzeb Policji, podlegały usunięciu, jeśli nie są już konieczne do celów, dla których zostały zarejestrowane.

W tym celu należy brać zwłaszcza pod uwagę następujące kryteria: konieczność zachowania danych w świetle wniosków wynikających z postępowania śledczego; ostateczne postanowienie sądu, a zwłaszcza uniewinnienie; rehabilitację; przedawnienie; amnestię; wiek osoby, której dane dotyczą; szczególne kategorie danych.

7.2. Należy ustanowić - w porozumieniu z organem nadzorczym, bądź zgodnie z prawem krajowym - reguły służące określaniu czasu i okresu przetwarzania różnych kategorii danych osobowych, jak również regularne kontrole ich jakości.

Zasada 8 - Bezpieczeństwo danych

Organ odpowiedzialny winien podejmować wszelkie środki konieczne do zagwarantowania danym odpowiedniego bezpieczeństwa fizycznego i logicznego, jak również do uniemożliwienia dostępu do tych danych i ich przekazywania osobom nieupoważnionym oraz dokonywania w nich zmian.

W tym celu, należy brać pod uwagę charakter zbiorów i ich różną zawartość.

MEMORANDUM WYJAŚNIAJĄCE

Wstęp

1. Mimo, iż zasady ochrony danych określone w Konwencji o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych (znanej jako Konwencja o Ochronie Danych) z dnia 28 stycznia 1981 roku odnoszą się ogólnie do gromadzenia, przetwarzania, wykorzystywania itd. danych osobowych zarówno w sektorze prywatnym, jak i publicznym, zaistniała konieczność przystosowania ich do specyficznych wymogów poszczególnych sektorów.

2. To „sektorowe ujęcie" ochrony danych doprowadziło do przyjęcia przez Komitet Ministrów Rady Europy czterech rekomendacji opracowanych przez międzyrządową Komisję Ekspertów ds. Ochrony Danych (CJ-PD): Rekomendacja Nr R(81)1 dotycząca automatycznych banków danych medycznych (z dnia 23 stycznia 1981 r.), Rekomendacja Nr R(83)10 o ochronie danych osobowych wykorzystywanych do celów naukowych i badań statystycznych (z dnia 23 września 1983 r.), Rekomendacja Nr R (85) 20 o ochronie danych osobowych wykorzystywanych dla celów marketingu bezpośredniego (z dnia 25 października 1985 r.) i Rekomendacja Nr R(86)1 o ochronie danych osobowych wykorzystywanych dla celów ubezpieczenia społecznego (z dnia 23 stycznia 1986 r.).

3. W ramach tego ujęcia sektorowego, w opinii Komisji Ekspertów ds. Ochrony Danych należało rozważyć problemy ochrony danych wynikające z wykorzystywania danych osobowych w sektorze Policji z zamiarem przygotowania instrumentu określającego zasady regulujące gromadzenie, przechowywanie, wykorzystywanie, przekazywanie i zachowywanie danych osobowych przez Policję. Powyższe zasady miały być inspirowane przepisami Konwencji o Ochronie Danych.

4. Biorąc pod uwagę rosnący udział sił policyjnych w życiu jednostek wynikający z nowych zagrożeń, jakie niosą dla społeczeństwa terroryzm, przestępstwa związane z narkotykami, itd., a także ogólny wzrost przestępczości, tym bardziej konieczne stało się ustalenie dla sektora Policji wyraźnych wytycznych, które określałyby niezbędną w naszych społeczeństwach równowagę pomiędzy prawami jednostek a prawnie uzasadnionymi działaniami Policji w zakresie wykorzystywania technik przetwarzania danych.

5. Pamiętając, iż treść Artykułu 9 ustęp 2 Konwencji pozwala Państwom Członkowskim na uchylanie podstawowych przepisów Konwencji o Ochronie Danych w celu, między innymi „zwalczania przestępstw", Komisja Ekspertów upoważniła grupę roboczą do określenia problemów wynikających z wykorzystywania danych osobowych w sektorze Policji i do sformułowania konkretnych propozycji ich rozwiązania. W skład grupy roboczej wchodzili eksperci z Belgii, Francji, Włoch, Holandii, Portugalii, Szwecji, Szwajcarii i Zjednoczonego Królestwa. Pod przewodnictwem dr R. Schweizera (Szwajcaria) grupa robocza spotkała się pięciokrotnie.

6. Podczas pierwszego posiedzenia (w dniach 19 i 20 grudnia 1983 roku) grupa robocza dokonała próby zidentyfikowania zakresu, w jakim ustawodawstwo Państw Członkowskich reguluje w szczególności przepis o wykorzystywaniu danych osobowych w sektorze Policji. Ponadto uzyskano szeroki obraz problematyki, jaką stwarza ten sektor dla ochrony danych. Zadanie grupy roboczej zostało ułatwione przez opracowanie przygotowane przez konsultanta, profesora H. Maisl (Francja).

7. Podczas drugiego spotkania (w dniach 18–20 czerwca 1984 roku) członkowie grupy roboczej kontynuowali prace nad wyżej wymienionymi tematami, uwzględniając tym razem odpowiedzi Państw Członkowskich na pytania zawarte w kwestionariuszu. Ponadto, grupa robocza dokonała analizy stosownego prawa precedensowego Trybunału Europejskiego i Europejskiej Komisji Praw Człowieka w kontekście Artykułu 8 Europejskiej Konwencji o Ochronie Praw Człowieka, a mającego związek z gromadzeniem, wykorzystywaniem, przechowywaniem, itd. danych osobowych przez Policję. Dyskusje zaowocowały powstaniem wstępnego projektu instrumentu prawnego, będącego odzwierciedleniem tymczasowych opinii grupy roboczej na temat sposobów prawnej regulacji wykorzystywania danych osobowych w sektorze Policji.

8. Na trzecim posiedzeniu (w dniach 17-19 grudnia 1984 roku) grupa robocza przystąpiła do nowelizacji projektu wstępnego. Rozważano w szczególności zakres wyłączeń określonych w Artykule 9 ustęp 2 Konwencji o Ochronie Danych. Grupa robocza kontynuowała prace stojąc na stanowisku, iż należy ustalić zbiór przepisów o ochronie danych z myślą o podstawowych i kluczowych zadaniach Policji, które jednocześnie uwzględniałyby szczególne wymagania, zwłaszcza w odniesieniu do „zwalczania przestępstw".

9. W oparciu o komentarze i obserwacje przedstawione przez komisję plenarną informowaną na bieżąco o postępie prac, grupa robocza podczas kolejnych spotkań (w dniach 5-7 czerwca 1985 roku i 27-29 listopada 1985 roku) rozszerzyła zakres dokonywanej analizy o tematy takie, jak przekazywanie przez Policję danych osobowych osobom trzecim, a zwłaszcza przekazywanie danych za granicę. Tekst ostateczny został przekazany komisji plenarnej razem z projektem memorandum wyjaśniającego przygotowanym przez Sekretariat.

10. Na 13 posiedzeniu (w dniach 4-7 listopada 1986 roku) Komisja Ekspertów, po dokonaniu analizy, zatwierdziła projekt Rekomendacji i projekt memorandum wyjaśniającego oraz podjęła decyzję o przedstawieniu tych tekstów Europejskiej Komisji ds. Współpracy Prawnej (CDJC) w celu dokonania ich oceny i zatwierdzenia.

11. Projekty Rekomendacji i memorandum wyjaśniającego zostały zatwierdzone przez Europejską Komisję Współpracy Prawnej w dniu 22 maja 1987 roku.

12. Rekomendacja Nr R(87)15, regulująca wykorzystywanie danych osobowych w sektorze Policji została przyjęta przez Komitet Ministrów Rady Europy w dniu 17 września 1987 roku.

Komentarz szczegółowy

Preambuła

13. Niewątpliwie nowoczesna technologia ułatwia pracę Policji. W sektorze, w którym gromadzenie i przetwarzanie dużej ilości danych osobowych jest nieodzowne w świetle szerokiego zakresu działań i ważnej społecznie roli sił policyjnych, korzyści wypływające z wykorzystywania nowych technologii są oczywiste. Coraz bardziej wyrafinowana przestępczość wymaga równoważnych, równie wyrafinowanych metod egzekwowania prawa. Komputery w szczególności pozwoliły Policji zwiększyć efektywność przy gromadzeniu i przechowywaniu danych osobowych, a także przyczyniają się do szybszego podejmowania decyzji w zakresie egzekwowaniu prawa dla dobra społeczeństwa.
14. Jednakże niepokój, który przyspieszył opracowanie Konwencji o Ochronie Osób w Związku

z Automatycznym Przetwarzaniem Danych Osobowych z dnia 28 stycznia 1981 roku najdotkliwiej jest odczuwalny w sektorze Policji. Jest to bowiem dziedzina, w której pogwałcenie podstawowych zasad określonych we wspomnianej Konwencji może istotnie zaciążyć na życiu jednostki.

15. Preambuła zawiera stwierdzenie o potrzebie zachowania równowagi pomiędzy interesami zaangażowanych stron – interesu jednostki, jej prawem do ochrony prywatności a interesami społeczeństwa w zakresie zapobiegania i zwalczania przestępstw oraz utrzymywaniu porządku publicznego.

16. Nic więc dziwnego, iż równowaga taka jest niezmiernie trudna do osiągnięcia w sektorze Policji. Zarówno Artykuł 8 ustęp 2 Europejskiej Konwencji o Ochronie Praw Człowieka, jak i Artykuł 9 Konwencji o Ochronie Danych, dopuszczają istnienie wyjątków od gwarantowanych praw.

17. Mimo, iż preambuła odnosi się do możliwych zagrożeń prywatności jednostek w trakcie niewłaściwego wykorzystywania metod automatycznego przetwarzania, należy pamiętać, iż prywatności nie można interpretować jedynie w ramach ochrony prywatnej sfery życia przed postępowaniem godzącym w czyjeś prawa. Z tego właśnie powodu preambuła zwraca uwagę na Artykuł 8 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności oraz na legalność pewnych technik inwigilacji, co oznacza, iż uzyskanie danych od osób fizycznych musi podlegać przepisom Artykułu 8 i odpowiednim orzeczeniom Europejskiego Trybunału Praw Człowieka.

18. Działania polegające na zakładaniu podsłuchów i przejmowaniu korespondencji stanowią *sensu stricto* przykład ingerencji w życie prywatne. Europejski Trybunał Praw Człowieka wydał dwukrotnie orzeczenia w takich sprawach (sprawa Klassa i innych, wyrok z dnia 6 września 1978 roku, Seria A, nr 28; sprawa Malone, wyrok z dnia 2 sierpnia 1984 roku, Seria A, nr 82). Zasada 2 pkt 2.2. i 2.3. muszą być interpretowane w świetle prawa precedensowego Trybunału.

19. Jednakże preambuła odnosi się również do przepisów Konwencji o Ochronie Osób w Związku z Automatycznym Przetwarzaniem Danych Osobowych z dnia 28 stycznia 1981 roku, które wychodzą poza tradycyjne pojęcia prywatności i określają zestaw podstawowych zasad ochronnych mających na celu regulację prawną gromadzenia, przechowywania, wykorzystywania i przekazywania danych osobowych.

20. W preambule zawarte jest szczególne odniesienie do derogacji z mocy Artykułu 9 Konwencji o Ochronie Danych. Przypominamy, iż uchylenia przepisów Artykułu 5 („jakość danych"), Artykułu 6 (zasady dotyczące „szczególnych kategorii danych") i Artykułu 8 („dodatkowe zabezpieczenia osoby, której dane dotyczą") są właściwe jedynie wtedy, gdy wynikają z mocy prawa i stanowią w demokratycznym społeczeństwie środek konieczny w celu, między innymi, zwalczania przestępstw. Mając na uwadze fakt, iż Europejski Trybunał Praw Człowieka w treści wyroku w sprawie Malone wskazał wyraźnie te kryteria (precyzja, pewność, przewidywalność, itd.) można przyjąć, iż zasady zawarte w tym nieobowiązującym instrumencie prawnym, mogą dla ustawodawcy stanowić źródło wytycznych, co do interpretacji uchyleń z mocy Artykułu 9 ustęp 2 Konwencji o Ochronie Danych w odniesieniu do przepisów regulujących gromadzenie, wykorzystywanie, itd. danych osobowych w sektorze Policji. Należy o tym pamiętać, na przykład w kontekście brzmienia Zasady 2 pkt 2.1.

21. Jak już wspomniano, zakres derogacji jest węższy, niż interes społeczny opisany w ustępie 5

preambuły. Jednakże celem niniejszej Rekomendacji jest utworzenie zbioru przepisów o ochronie danych osobowych wykorzystywanych dla realizacji podstawowych i kluczowych zadań Policji przy jednoczesnej adaptacji wspomnianych przepisów tak, aby uwzględniały oczekiwania społeczeństwa zwłaszcza w stosunku do „zwalczania przestępstw". Oczywistym jest fakt, iż dane osobowe gromadzone i wykorzystywane dla zadań innych, niż typowe działania Policji, na przykład dla celów administracyjnych, są przedmiotem ogólnych norm dotyczących ochrony danych.

Zakres i definicje

22. Zgodnie z zamierzeniami przepisy regulują podstawowe fazy związane z ochroną danych – gromadzenie, przetwarzanie, wykorzystywanie i przekazywanie danych osobowych. Należy zaznaczyć, iż działania te są powiązane z pojęciem celowości, ujmowanej jako „cel policyjny". Ten ostatni termin jest definiowany w świetle interesów istotnych dla społeczeństwa, o czym wspomniano w punkcie piątym preambuły. Jednakże przypomnieć należy, iż określenie „celowość" będzie przedmiotem uszczegółowienia w dalszej części tekstu w celu zapewnienia, że w przepisach tych inaczej traktować się będzie zadania, które Policja musi wykonywać w związku ze zwalczaniem przestępstw, niż zadania na poziomie prewencji i utrzymywania porządku publicznego.

23. Niniejsza Rekomendacja dotyczy jedynie władz policyjnych. Należy pamiętać, iż w zależności od systemu prawnego, współistnieć mogą różne służby policyjne. Z punktu widzenia podziału pracy i obowiązków nie zawsze można je łatwo odróżnić od siebie. Jednakże, bez względu na nazewnictwo, przepisy te stosuje się do każdego organu sprawującego funkcje Policji, związane jednocześnie z gromadzeniem, przechowywaniem, wykorzystywaniem i przekazywaniem danych osobowych do celów określonych w ustępie trzecim tej części dokumentu.

24. Niniejsza Rekomendacja odnosi się głównie do zautomatyzowanych danych osobowych, a termin „dane osobowe" jest definiowany w sposób zgodny z zakresem, w jakim był stosowany w innych rekomendacjach Rady Europy dotyczących ochrony danych. Warto powtórzyć, iż decyzja o tym, czy jednostka ma być uznana za „możliwą do zidentyfikowania" lub też nie, winna być podejmowana obiektywnie. Przy czym należy uwzględnić różnorodność metod identyfikacji stosowanych przez Policję, jak na przykład, techniki daktyloskopijne, systemy rozpoznawania głosu, inwigilacji baz danych ... etc.

25. „Organem odpowiedzialnym" jest, wykorzystując terminologię Konwencji, administrator zbioru danych ponoszący całkowitą odpowiedzialność za administrowany zbiór. Zgodnie z Zasadą 1 pkt 1.4. do organu nadzorczego należy zgłaszać nazwę organu odpowiedzialnego za poszczególne zbiory.

26. Mimo, iż zakres tego instrumentu prawnego jest ograniczony do zautomatyzowanych danych osobowych – jak to ma miejsce w przypadku ustawodawstwa niektórych Państw Członkowskich Rady Europy - należy pamiętać, iż w wielu z tych państw wciąż bazuje się na zbiorach manualnych. Ponadto w krajach, gdzie komputeryzacja Policji jest wysoko zaawansowana, dane magazynowane w komputerach mogą być odczytane jedynie wtedy, gdy zostanie dokonane odniesienie do zbiorów manualnych. W związku z powyższym, nie należy wyłączać zbiorów ręcznych z zakresu niniejszych przepisów i z tego powodu niniejszy instrument prawny zezwala Państwom Członkowskim na obejmowanie tymi przepisami również danych przetwarzanych w zbiorach manualnych. Paragraf 38 zawiera wytyczne określające stanowisko Państw Członkowskich wobec zagadnienia zbiorów

danych przetwarzanych ręcznie.

27. Oczywistym jest fakt, iż z upływem czasu coraz więcej danych, które obecnie są przechowywane w formie manualnej, będzie automatyzowanych i przepisy zawarte w niniejszym instrumencie prawnym obejmą w przyszłości również te dane. Jednak nie powinno się zezwalać Państwom Członkowskim na świadome obchodzenie gwarancji, jakie niesie ten instrument prawny, poprzez przekazywanie danych osobowych ze zbiorów zautomatyzowanych do zbiorów ręcznych. Tym niemniej mogą pojawić się trudności w określeniu, czy zaistniało świadome obejście w przypadku, gdy dane są usuwane zgodnie z Zasadą 7, ale wydruk tych danych jest zachowany.

28. Zgodnie z Artykułem 3 ustęp 2 Konwencji o Ochronie Danych przyjmuje się, że Państwa Członkowskie stosują te zasady do osób prawnych.

29. Ostatecznie, jeśli chodzi o kwestie bezpieczeństwa państwa, które raport wyjaśniający do Konwencji o Ochronie Danych opisuje jako „ochronę suwerenności narodowej przed wewnętrznymi i zewnętrznymi zagrożeniami, nie wyłączając ochrony międzynarodowych stosunków państwa", pożądane jest, aby uznać swobodę Państw Członkowskich w zakresie rozszerzania niektórych zabezpieczeń określonych w niniejszym instrumencie prawnym na dziedziny związane z bezpieczeństwem państwa wszędzie tam, gdzie ich zastosowanie wydaje się być stosowne i możliwe do przeprowadzenia.

30. Oprócz poszczególnych zagadnień związanych z bezpieczeństwem państwa i osób prawnych, pamiętać należy, iż Zasady określone w niniejszej Rekomendacji uważane były przez jej projektodawców za zabezpieczenia minimalne oraz to, że Państwa Członkowskie zachowały wolność ustalania silniejszych środków ochrony.

Zasada 1 – kontrola i zawiadomienia

31. W ramach krajowych ustaw o ochronie danych główną rolę odgrywają organy ochrony danych oraz rzecznicy. Wszędzie tam, gdzie władze takie istnieją należy im powierzyć zadania określone w niniejszej Rekomendacji. Niepożądanym byłoby utworzenie odrębnego, konkurującego organu dla celów niniejszej Rekomendacji. Jednakże każdy nowo utworzony organ winien być faktycznie niezależny od kontroli Policji. Jest to podstawowa właściwość biorąc pod uwagę, iż niniejsza Rekomendacja zakłada możliwość przekazania kompetencji podejmowania decyzji, w tym także ocenę ograniczeń nałożonych na działania Policji odnośnie danych osobowych, temu właśnie organowi.

32. Struktura ustrojowa niektórych Państw Członkowskich może nakładać obowiązek utworzenia kilkunastu niezależnych organów władzy nadzorczej w sytuacji, gdy organy ochrony danych lub rzecznicy ochrony danych osobowych jeszcze nie istnieją. Ciało takie nie musi koniecznie być ciałem kolegialnym. Umożliwiałoby to osobie fizycznej spełnianie roli „gwarantującego poszanowanie Zasad zawartych w niniejszej Rekomendacji". Jednakże biorąc pod uwagę, jak ważna jest to rola, pożądanym byłoby, aby organ nadzorczy, bez względu na formę, posiadał wystarczające środki do efektywnego działania.

33. Ostatecznie, należy zaznaczyć, iż brak ogólnego ustawodawstwa dotyczącego ochrony danych nie stanowi przeszkody w tworzeniu niezależnego organu nadzorczego dla sektora Policji. Zasady zawarte w niniejszej Rekomendacji są adresowane do wszystkich Państw Członkowskich i mogą być przyjęte również przez kraje, które dopiero będą przyjmować ogólne normy ochrony danych.

34. W preambule zawarte jest stwierdzenie, iż wraz z rozwojem komputeryzacji, nowe techniczne środki przetwarzania danych, takie jak na przykład systemy rozpoznawania głosu, mechaniczne czytniki kart identyfikacyjnych, komputerowe techniki inwigilacji, czy elektroniczne systemy namierzania stały się bardzo użyteczne w pracy Policji. Jednakże, uwzględniając możliwość ich niewłaściwego wykorzystywania, podstawowego znaczenia nabiera konieczność zapewnienia, aby ich wprowadzanie i wykorzystywanie odbywało się ze świadomością ich ogromnego wpływu na życie jednostek. Zasada 1 pkt 1.2. zaleca zwrócenie szczególnej uwagi na sposób ich wprowadzania oraz zagwarantowania, że nie będą one godzić w ducha istniejącego prawa o ochronie danych. Ponadto pożądana wydaje się być publiczna debata na temat wprowadzania nowych technologii, które mogą stanowić dla prywatności poważne zagrożenie, niezamierzone przez ustawodawcę w chwili ustanawiania norm ochrony danych.

35. W tym znaczeniu niezależny organ nadzorczy ma do spełnienia istotną rolę. Zgodnie z Zasadą 1 pkt 1.3. winien on posiadać kompetencje do przeprowadzenia obserwacji na prośbę organu odpowiedzialnego, który zamierza wprowadzić zautomatyzowane metody przetwarzania danych, co może rodzić problemy wobec zastosowania niniejszej Rekomendacji. Punkt 1.3. nie przewiduje prawa *veta* wobec takiego wprowadzenia. Jednakże zezwala organowi nadzorczemu na sprawdzenie proponowanych metod w celu określenia czy, na przykład, przy ich stosowaniu nie będą omijane wytyczne dotyczące przekazywania danych (Zasada 5). Zezwala również organowi nadzorczemu na udzielanie porad organowi odpowiedzialnemu w zakresie podjęcia środków mających zagwarantować poszanowanie zasad niniejszej Rekomendacji.

36. Dla potrzeb niniejszego dokumentu, zbiory policyjne obejmują wszystkie uporządkowane/zorganizowane dane osobowe, które przetwarzane są przez służby policyjne w celu wypełnienia zobowiązań w zakresie prewencji, zwalczania przestępstw i utrzymywania porządku publicznego. Tak zdefiniowane zbiory policyjne umożliwiają Policji uzyskiwanie informacji odnoszących się do osób zidentyfikowanych bądź możliwych do zidentyfikowania. Zasada 1 pkt 1.4. zobowiązuje Policję lub inne organy wyznaczone przez prawo krajowe do zgłaszania swych zautomatyzowanych zbiorów do organów nadzorczych i określenia szczegółów dotyczących każdego z tych zbiorów.

37. Należy zauważyć, iż obowiązek zgłoszenia jest natury ogólnej. Nie sformułowano żadnych wyjątków na korzyść zbiorów związanych jedynie ze zwalczaniem przestępstw. Jak już wspomniano, niniejsza Rekomendacja jest próbą ustalenia szczegółowych zasad ukierunkowanych na klasyczne zadania Policji, odbiegając od nich tylko w przypadku, gdy konieczne jest uwzględnienie szczególnych zadań Policji w zakresie „zwalczania przestępstw".

38. Mimo, że przepis dotyczący zgłoszenia ogranicza się do zautomatyzowanych zbiorów danych, może zaistnieć przypadek, iż niektóre Państwa Członkowskie skorzystają z prawa rozszerzenia przepisów sformułowanych w niniejszym instrumencie prawnym na zbiory policyjne przetwarzane manualnie. Wówczas Państwo Członkowskie może zobowiązać Policję do przechowywania opisu każdego typu zbioru przetwarzanego ręcznie zawierającego informacje o administratorze takiego zbioru, celu, dla jakiego go utworzono, rodzaju zawartych w nim danych i o osobach, którym dane są przekazywane. Taki ogólny opis podlegałby zgłoszeniu do organu nadzorczego. W innej sytuacji można by uniknąć konieczności zgłaszania każdego opisu zbioru, gdyby wymagano od każdego z oddziałów Policji zagwarantowania, że ręcznie przetwarzane przez niego zbiory są zgodne z opisem ustalonym na poziomie centrali. Jeśli oddział Policji nie podporządkuje się temu opisowi, może zostać zobowiązany do utworzenia własnego opisu i zgłoszenia go do organu nadzorczego.

39. Możliwe są inne sposoby rozszerzenia niniejszych zasad na zbiory przetwarzane ręcznie.

40. Drugi podpunkt Zasady 1 pkt 1.4. dotyczy zagadnienia zbiorów doraźnych tworzonych *ad hoc* na potrzeby toczącego się śledztwa.

Zgłaszanie każdego zbioru tworzonego *ad hoc* mogłoby powodować niepotrzebną biurokrację. Jednak i takie zbiory nie powinny uniknąć jakiejś formy zgłoszenia. Prawo krajowe może określać okoliczności, w których informacje o takich zbiorach przedstawiane byłyby organowi nadzorczemu. Istnieje również możliwość, aby prawo krajowe wymagało zgłoszenia jedynie faktu istnienia zbiorów *ad hoc*, lub też ogólnego zgłoszenia zawierającego określenie ich typów, zezwalając organowi nadzorczemu na prowadzenie dochodzenia w celu ustalenia, czy tworzenie takich zbiorów jest zgodne z przepisami o ochronie danych.

41. W sytuacji, gdy nie istnieją wytyczne w prawie krajowym, organ nadzorczy we współpracy z organem odpowiedzialnym, o którym wspomniano wcześniej, może opracować przepisy o zgłaszaniu zbiorów *ad hoc*. Na przykład, z porozumienia pomiędzy organem nadzorczym a organem odpowiedzialnym może wyniknąć, że zbiory takie powinny być zgłoszone do rejestracji zarówno po upływie uzasadnionego czasu ich istnienia, jak i gdy domniemywa się, że będą one przez ten uzasadniony czas istniały. Inne kryteria zgłaszania zostaną określone.

42. Zbiory powstałe dla celów pojedynczego śledztwa, podlegające szybkiemu zniszczeniu po jego zakończeniu, nie wymagają zgłoszenia.

Zasada 2 - Gromadzenie danych

43. Zasada 2 pkt 2.1. wyklucza możliwość gromadzenia przez Policję danych na bieżąco i bez rozróżniania kategorii danych. W ten sposób wyrażone zostało jakościowe i ilościowe ujęcie Artykułu 5.c. Konwencji o Ochronie Danych, który określa, że dane osobowe muszą być odpowiednie, istotne oraz nie wykraczające poza potrzeby wynikające z celów, dla których zostały zarejestrowane. Uwzględniając fakt, że Artykuł 9.a. Konwencji zezwala na uchylenie powyższego przepisu w przypadku „zwalczania przestępstw", Zasada 2 pkt 2.1. niniejszej Rekomendacji jest próbą określenia granic tego rodzaju wyjątków poprzez ograniczenie gromadzenia danych osobowych tylko do sytuacji, w których jest to niezbędne dla zapobiegania realnym niebezpieczeństwom lub zwalczaniu konkretnych przestępstw i o ile prawo krajowe nie sankcjonuje szerszych kompetencji Policji do gromadzenia informacji. Terminu „realne niebezpieczeństwa" nie należy rozumieć, jako ograniczonego jedynie do konkretnego przestępstwa lub przestępcy, ale wyłączając bezpodstawne spekulacje należy uwzględnić także okoliczności, w których istnieje uzasadnione podejrzenie, że poważne przestępstwo zostało lub zostanie popełnione. Jako przykład można tu podać reakcję Policji na uzasadnione podejrzenie, iż bliżej nieokreślone narkotyki są nielegalnie wwożone do jakiegoś kraju drogą morską na pokładzie prywatnych jachtów. Usprawiedliwiałoby to zbieranie przez Policję danych o wszystkich jachtach korzystających z tego portu, ale nie o wszystkich jachtach, ich właścicielach i pasażerach w każdym porcie w tym kraju.

44. Zasada 2 pkt 2.2. dotyczy gromadzenia i przechowywania danych bez wiedzy osoby, której dane dotyczą i stanowi próbę regulacji przypadków, w których podjęto decyzję o zachowaniu danych uzyskanych bez wiedzy tej osoby. Osoba ta winna być poinformowana, że jej dane są przechowywane w takiej formie, jak tylko zmaleje prawdopodobieństwo

poniesienia przez przedmiot działań Policji jakiejkolwiek szkody. Oczywiście procedura ta nie będzie konieczna, jeśli Policja podejmie decyzję o usunięciu danych zebranych bez wiedzy danej osoby.

Przyjmuje się, iż Zasada 2 pkt 2.2. może okazać się trudna do zrealizowania tam, gdzie w grę wchodzi wykorzystywanie kamer video instalowanych na ulicach, czy użycie innych podobnych metod inwigilacji masowej, umożliwiającej zbieranie informacji o dużej liczbie osób. Z tego powodu przepis ten zawiera wskazanie, aby tych, którzy mogą być obiektem tajnej obserwacji poinformować o tym fakcie, gdy tylko stanie się to wykonalne.

45. Uważa się, że Państwa Członkowskie mogą uznać tę zasadę za szczególnie ważną pamiętając, że prawo precedensowe Europejskiej Komisji Praw Człowieka, która w kontekście Artykułu 8 Europejskiej Konwencji o Ochronie Praw Człowieka uznaje, że gromadzenie i przechowywanie danych dotyczących jednostki bez jej zgody może rodzić problemy związane z ochroną danych (Skarga Nr 8170/78,X v. Austria, Skarga Nr 9248/81. Leander v. Szwecja).

46. Pkt 2.2. Zasady 2 kładzie nacisk na przechowywanie danych osobowych zebranych bez wiedzy osoby, której one dotyczą przy wykorzystaniu zarówno tajnych, jak i jawnych środków (na przykład zadawanie pytań sąsiadom osoby, której dane dotyczą), a pkt 2.3. jest ukierunkowany na zbieranie danych przy pomocy technicznej inwigilacji i innych metod zautomatyzowanych. Zbieranie danych takimi metodami winny regulować w prawie krajowym odrębne przepisy. W szczególności należy pamiętać o prawie precedensowym Europejskiego Trybunału Praw Człowieka, gdy odnosimy się do zakładania podsłuchów. Orzeczenie Trybunału w sprawie Malone stanowi, iż taka forma technicznej inwigilacji musi być precyzyjnie autoryzowana przez dostępne przepisy prawne, które określą zakres i sposób podejmowania decyzji przez odpowiednie władze oraz odpowiednie zabezpieczenia przed ewentualnymi nadużyciami.

47. Organy egzekwowania prawa działają w granicach ustawowych i wszelkie ich działania związane z pozyskiwaniem danych podlegają tym samym ograniczeniom. Zgodnie z powyższym, należy respektować krajowe przepisy prawne, bazujące co najmniej na przepisach Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (1950). W tym zakresie należy uwzględniać również prawo precedensowe Europejskiej Komisji i Europejskiego Trybunału Praw Człowieka dotyczące aresztowania i tymczasowego zatrzymania w celu przesłuchania, przeszukania i zajęcia, metod przesłuchań, pobierania próbek, odcisków palców i fotografowania, itd. To oczywiste, że odpowiednie prawodawstwo krajowe musi odpowiadać przepisom Konwencji zgodnie z interpretacją Europejskiego Trybunału Praw Człowieka.

48. Pkt 2.4. omawia zagadnienie danych szczególnie chronionych i wyraża opinię zawartą w Artykule 6 Konwencji o Ochronie Danych, iż zbieranie i przechowywanie szczególnych kategorii danych winno podlegać ograniczeniom. Może zaistnieć sytuacja, iż zbieranie pewnych danych szczególnie chronionych będzie niezbędne dla celów określonych w punkcie 2.1. Zasady 2. Jednakże w żadnych okolicznościach dane takie nie powinny być zbierane tylko po to, aby umożliwić Policji opracowanie zbioru dotyczącego jakiejś grupy mniejszościowej, której zachowanie mieści się w granicach prawa. Zbieranie takich danych jest zgodne z prawem tylko wtedy, jeśli jest „absolutnie konieczne dla wypełnienia celów konkretnego śledztwa". Wyrażenie „konkretne śledztwo" należy traktować jako

ograniczenie ogólne. Śledztwo takie winno opierać się na umotywowanym przekonaniu osób je prowadzących, iż poważne przestępstwo zostało lub może być popełnione. Ponadto zbieranie danych szczególnie chronionych w takich okolicznościach winno być „absolutnie konieczne" dla potrzeb takiego śledztwa.

Powyższego nie stosuje się do danych dotyczących zachowań seksualnych, gdy popełniono przestępstwo.

Zasada 3 – Przechowywanie danych

49. Zebrane dane osobowe będą następnie podlegały decyzjom dotyczącym ich przechowywania w zbiorach policyjnych. Zasada 3 pkt 3.1. określa wymagania wobec ograniczeń dokładności i przechowywania danych. Przechowywane dane powinny być dokładne i powinny się ograniczać do danych koniecznych do tego, by umożliwić organom policyjnym wypełnienie zgodnych z prawem zadań. Z treści Zasady 3 pkt 3.1. wynika, iż nie tylko prawo krajowe, ale także prawo międzynarodowe, które dla celów niniejszej Rekomendacji obejmuje również współpracę międzynarodową w ramach Interpolu, może również być źródłem działań Policji zgodnych z prawem (na przykład, międzynarodowe umowy prawne o współpracy pomiędzy oddziałami Policji w różnych krajach), co uzasadnia przechowywanie danych.

50. Przepis ten jest ważny biorąc pod uwagę fakt, że przekazywanie danych osobowych do zbiorów policyjnych może doprowadzić do powstania stałego rejestru, a masowe przechowywanie danych może naruszyć prawa i wolności jednostki. W interesie Policji jest również to, aby w swych zbiorach posiadała tylko dokładne i rzetelne dane.

51. Należy zauważyć, iż Zasada 3 jako całość stanowi przepis ogólny odnoszący się do wszystkich rodzajów danych zbieranych dla celów Policji zgodnie z wcześniejszą definicją.

52. Treść pkt 3.2. stanowi zachętę do wprowadzania sytemu klasyfikacji danych. Uważa się, iż powinna istnieć możliwość rozróżnienia pomiędzy potwierdzonymi a niepotwierdzonymi danymi, dotyczy to także oceny zachowań ludzkich, faktami a opiniami, wiarygodnymi informacjami (a także różnymi ich rodzajami) a przypuszczeniami, pomiędzy uzasadnionym przekonaniem, że informacja jest dokładna a bezpodstawną wiarą w jej dokładność.

53. Dane zbierane i przechowywane przez Policję dla celów administracyjnych (na przykład informacje o wydanych pozwoleniach na broń lub o rzeczach zagubionych, itd.) podlegają oczywiście ogólnym przepisom o ochronie danych. W treści pkt 3.3. zawarte jest zalecenie, aby takie dane były przechowywane oddzielnie od danych przechowywanych dla celów policyjnych w rozumieniu niniejszego instrumentu prawnego, jeśli podjęto decyzję o zachowaniu ich na czas nieokreślony. Biorąc pod uwagę szczególne podejście do ochrony danych w sektorze Policji błędem byłoby w zasadzie zezwalanie, aby obejmować ścisłą kontrolą również dane administracyjne.

54. Jednakże zapewnienie ścisłego podziału pomiędzy tymi dwoma typami danych może nie zawsze być możliwe do przeprowadzenia. W takim przypadku Państwa Członkowskie winny dokonać oceny środków, jakie mogą być podjęte w celu zagwarantowania, aby dane administracyjne nadal podlegały ogólnym zasadom ochrony danych.

Zasada 4 - Wykorzystywanie danych przez Policję

- Zasada 4 określa wyraźnie pojęcie celowości: dane osobowe zbierane dla celów związanych z prewencją i zwalczaniem przestępstw oraz utrzymywaniem porządku publicznego mogą być wykorzystywane jedynie do tych celów. Jednakże bezwarunkowy charakter tego przepisu uległ częściowej modyfikacji w treści Zasady 5.

Zasada 5 – Udostępnianie danych

56. Zasada 5 jest zbudowana tak, aby w sposób odrębny regulować różnorodne formy zgodnego z prawem udostępniania danych, przy jednoczesnym określeniu przepisów ogólnych odnoszących się do wszystkich przewidywanych udostępnień.

57. Udostępnianie danych w ramach sektora Policji jest uwarunkowane otrzymaniem od Policji upoważnienia potwierdzającego zgodną z prawem potrzebę uzyskania danych, na przykład, gdy odbiorca danych potrzebuje ich dla celów związanych z prewencją i zwalczaniem przestępstw oraz utrzymywaniem porządku publicznego. Przyjmuje się, że organ Policji ubiegający się o informacje u innego organu Policji może udostępnić pewne dane tak, aby żądanie pozyskania informacji zostało wypełnione pod warunkiem, że obie strony udostępnienia spełniają prawnie uzasadnione wymagania określone w punkcie 5.1.

58. Biorąc pod uwagę, iż udostępnianie danych może *sensu stricto* odbywać się dla celów nie związanych z działalnością Policji, poza obszarem udostępniania danych w ramach tego sektora warunki udostępniania są już bardziej rygorystyczne. Zwraca uwagę wyjątkowy charakter okoliczności, w których zezwala się na udostępnienie danych na warunkach przedstawionych w punktach 5.2. i 5.3. Podkreślić należy, iż za szczególnie wyjątkowe uważa się sytuacje opisane w podpunktach a. i b. obydwu punktów 5.2.ii. oraz 5.3.ii. Zasady 2.

59. Organami publicznymi, o których mowa w punkcie 5.2. mogą być, na przykład, zakłady ubezpieczeń społecznych lub urzędy podatkowe prowadzące dochodzenia w sprawach o oszustwo, urzędy imigracyjne, celne, itp.

60. Ogólne warunki udostępniania danych tym organom są określone w Zasadzie 5 pkt 5.2.i. ustęp a. i b. Należy podkreślić, iż w punkcie 5.2.i.a. przewidziana jest możliwość udzielania zezwolenia na udostępnianie danych przez organ nadzorczy. Mając na myśli taką rolę do spełnienia, w treści Zasady 1 podkreśla się potrzebę niezależności organu nadzorczego od sektora Policji.

„Wyraźne upoważnienie prawne” w odniesieniu do Zasady 5 pkt 5.2.i.a. może być udzielane przez sędziego.

61. Współpraca pomiędzy władzami policyjnymi a wyżej wspomnianymi organami jest również możliwa, gdy nie zaistnieją okoliczności, o których mowa w punkcie 5.2.i.a. Na przykład punkt 5.2.i.b. zezwalałby instytucji ubezpieczeń społecznych prowadzącej dochodzenie w sprawie o oszustwo na uzyskanie dostępu do odpowiednich danych policyjnych, jeśli są one niezbędne dla śledztwa. Powszechnie wiadomo, że gdy organy publiczne, o których mowa w punkcie 59 Memorandum, angażują się w działania podobne do działań Policji, posiadane przez nie informacje mogą mieć dla nich istotne znaczenie. Pojęcie niezgodności z celem pierwotnym, o którym mowa w punkcie 5.2.i.b. stanowi odniesienie do artykułu 5.b. Konwencji o Ochronie Danych. Wobec powyższego dane mogą być przekazywane jedynie dla celu związanego z działaniami pokrewnymi. „Zobowiązania prawne” Policji winny być interpretowane zgodnie z prawem krajowym.

62. Punkt 5.2.ii. określa dwie dodatkowe sytuacje usprawiedliwiające udostępnianie danych i należy tu podkreślić, że sytuacje takie mają charakter „wyjątkowy”. Ilustracją jednej z takich sytuacji może być przypadek, w którym zakład ubezpieczeń społecznych stojąc wobec roszczeń emigranta o zasiłek, wymógł weryfikację legalnego statusu tegoż emigranta w jednym ze zbiorów policyjnych w kraju jego pochodzenia. Działania takie leżą także w interesie wnioskodawcy. Uznano, że niebezpieczeństwo określone w punkcie 5.b. musi być poważne i bezpośrednio zagrażające. Przyjęto za właściwe ujmowanie w ten sposób niebezpieczeństwa, jako że punkt 5.2.ii. określa jedynie związek z wyjątkowymi przypadkami usprawiedliwiającymi udostępnienie danych. W przypadku, gdy zaistniało poważne, ale nie bezpośrednio zagrażające niebezpieczeństwo, udostępnienie danych może mieć miejsce zgodnie z postanowieniami określonymi w punkcie 5.2.ii.a.

63. Okazjonalnie może zaistnieć konieczność, aby Policja udostępniła dane organom prywatnym, chociaż nie na taką skalę, jak to jest przewidywane w przypadku współpracy Policji z innymi organami publicznymi. W niektórych przypadkach Policja będzie udostępniała bankom i sklepom dane o znanych oszustach lub informacje o skradzionych kartach kredytowych i czekach. Po raz kolejny punkt 5.3. uznaje powyższe działania za przypadki wyjątkowe wymagające wyraźnego zobowiązania prawnego lub upoważnienia (na przykład zgody sędziego), lub zgody organu nadzorczego. Gdy brak jest tych elementów, w treści punktu 5.3. zawarte jest powtórzenie tych samych warunków, jakie określone są w punkcie 5.2.ii.

64. Zrozumiałym jest, iż postanowienia zawarte w punktach 5.2. i 5.3. obejmują również rozpowszechnianie i przekazywanie do instytucji publicznych lub osób prywatnych portretów pamięciowych lub zdjęć osób podejrzanych, będących rezultatem zautomatyzowanego przetwarzania danych.

65. Punkt 5.4. odnosi się do międzynarodowego przekazywania danych policyjnych w ścisłym znaczeniu pomiędzy organami policyjnymi. Odniesienie do prawa międzynarodowego dotyczy jedynie umów międzynarodowych o współpracy w zakresie spraw karnych oraz w ramach współpracy z Interpolem. Ponadto zapis ten uwzględnia istnienie lub zawarcie umów pomiędzy sąsiadującymi państwami w celu usprawnienia transgranicznego przekazu danych pomiędzy różnymi organami Policji.

66. W odniesieniu do terminu „organy Policji”, uznano, iż w niektórych Państwach Członkowskich pewne rodzaje działań Policji mogą być wykonywane przez inne władze, które w ścisłym znaczeniu nie są „organami Policji”. Z drugiej jednak strony może zaistnieć przypadek, iż pewne funkcje, które - jak się powszechnie sądzi - należą do kompetencji Policji, w niektórych Państwach Członkowskich mogą być wypełniane przez nie-policyjne agencje.

67. Dla celów określonych w punkcie 5.4. termin „organy Policji” powinien być rozumiany w szerokim znaczeniu. Pytanie, które należałoby zadać brzmi: "czy organ wykonuje działania związane z prewencją i zwalczaniem przestępstw oraz utrzymywaniem porządku publicznego". Punkt 5.4. nie powinien być rozumiany jako wykluczający możliwość przekazywania danych do zagranicznych władz sądowniczych w sytuacji, gdy władze te wykonują funkcje odnoszące się do prewencji i zwalczania przestępstw. Oczywiste jest, że wymagania określone w punkcie 5.4. muszą być respektowane.

68. Transgraniczny przepływ danych osobowych pomiędzy organami Policji winien odbywać się na warunkach określonych w punktach a. lub b. Punkt 5.4.b. będzie miał zastosowanie, jeśli kraj odbiorcy danych nie jest członkiem Interpolu lub gdy nie istnieje umowa upoważniająca do dokonywania przekazania danych odbiorcy.

69. Treść punktu 5.4. odzwierciedla w pewnym zakresie postanowienia Artykułu 12 Konwencji o Ochronie Danych odnoszącego się do zagadnienia transgranicznego przepływu danych. Należy podkreślić, iż klauzula „pod warunkiem, że nie godzi to w unormowania krajowe dotyczące ochrony danych osoby, której dane dotyczą" jest odpowiednikiem zawartej w punkcie 3.a. Artykułu 12 Konwencji, koncepcji „ochrony równoważnej" w kraju adresata. Zgodnie z powyższym, organ wysyłający winien być przekonany o istnieniu odpowiedniego poziomu ochrony danych policyjnych w kraju adresata w przypadku, gdy organ wysyłający narzuci warunki dotyczące wykorzystywania danych w państwie odbiorcy (na przykład, co do okresu ich przechowywania), należy warunki takie respektować. Również punkty 5.4.a. i b. podlegają temu zastrzeżeniu.

70. Punkt 5.5. określa normy prawne, które regulują różnorodne formy przekazu wspomniane powyżej.

Ukierunkowując przepisy regulujące przekazywanie danych, autorzy Rekomendacji inspirowali się w pewnym zakresie postanowieniami zawartymi w dokumencie „Przepisy o międzynarodowej współpracy Policji i o wewnętrznej kontroli archiwów Interpolu". Ponadto w treści znajdziemy również odniesienia do Europejskiej Konwencji o Wzajemnej Pomocy w Sprawach Karnych z dnia 20 kwietnia 1959 roku.

71. Kryteria określone w punkcie 5.5.i. mają na celu zagwarantowanie, aby przekazywanie danych było zasadne. Nie wolno zapominać, iż punkt 5.1. zobowiązuje organ Policji ubiegający się o dane u innego organu policyjnego do posiadania prawnie uzasadnionej potrzeby uzyskania danych. Jednakże punkt 5.5.i. przewiduje zarówno wewnętrzną, jak i zewnętrzną wymianę danych będącą przedmiotem uzasadnionego wniosku.

72. Jednakże przepisy prawa krajowego lub postanowienia umów międzynarodowych mogą zwalniać z wymogu przedstawienia uzasadnionego wniosku.

73. Punkt 5.5.ii. w swej naturze nie jest zapisem bezwzględnym. Warunki w nim określone winny być spełnione „w miarę możliwości". Na przykład przyjmuje się, że w niektórych krajach decyzje sędziów nie zawsze są przekazywane do wiadomości organów Policji.

74. Jak to zostało stwierdzone wcześniej, w interesie obu stron, zarówno Policji, jak i osoby fizycznej jest, aby dane były adekwatne.

75. Punkt 5.5.ii. jest elastyczny w tym rozumieniu, iż uznaje istnienie w poszczególnych krajach różnych okresów monitorowania danych. Z tego też powodu weryfikacja jakości danych jest możliwa do momentu ich udostępnienia.

76. Punkt 5.5.iii. może wyjątkowo dopuszczać wykorzystywanie danych dla celów innych niż te uzasadniające pierwotny wniosek o udostępnienie. Istotne jest, aby organ przekazujący był poinformowany o takim zamiarze wykorzystywania danych. Należy pamiętać, iż różne cele muszą odnosić się do jednego lub więcej czynników wspomnianych w punktach od 5.2. do 5.4.

77. Punkt 5.5.iii. nie ma zastosowania do udostępniania danych w ramach sektora policyjnego. W tym przypadku zastosowanie mają regulacje określone w punktach 4.1. i 5.1.

78. O ile Zasada 2 stanowi ogólny zapis dotyczący zbierania danych przez Policję, to punkt 5.6. odnosi się do szczególnej sytuacji, w których Policja może zajmować się zbieraniem danych

łącząc zbiory własne ze zbiorami przechowywanymi dla innych celów, na przykład: instytucji ubezpieczeń społecznych, list pasażerów linii lotniczych, list członków związków zawodowych, itd. Ewentualnie można poszukiwać możliwości dopasowywania wielu zbiorów w celu ustalenia, czy zawierają one wyraźny rys pewnego rodzaju przestępstw oraz osób, które prawdopodobnie mogą być zamieszane w to przestępstwo.

79. Legalność takich praktyk jest uwarunkowana uzyskaniem jednego z wielu upoważnień opisanych w punktach a. i b. „Wyraźna klauzula prawna", o której wspomina się w punkcie 5.6.b. powinna określać warunki, po spełnieniu których może dojść do połączenia.

80. Możliwość, aby Policja posiadała bezpośredni dostęp przy użyciu komputerów do zbiorów przechowywanych przez inny organ policyjny lub inną instytucję, jest omówiona w ostatnim podpunkcie punktu 5.6. W tych okolicznościach dostęp bezpośredni musi być realizowany w zgodzie z ustawodawstwem krajowym będącym odzwierciedleniem podstawowych przepisów niniejszej Rekomendacji.

Zasada 6 – Publiczność informacji o istnieniu zbiorów policyjnych, prawo dostępu do zbiorów policyjnych, prawo do sprostowania i prawo do odwołania.

81. Fundamentalne znaczenie ma wymóg upublicznienia informacji o istnieniu zbiorów policyjnych, a także o prawach osób w odniesieniu do zbiorów policyjnych. Punkt 6.1. powierza organowi nadzorczemu zadanie podania do publicznej informacji, ale Państwa Członkowskie bez wątpienia znajdą dodatkowe sposoby wprowadzania tego wymogu w życie.

82. Wymóg rozpowszechniania w zasadzie winien być stosowany do wszystkich zbiorów zautomatyzowanych. Jednakże uznaje się, iż ilość informacji, która może być przekazywana Policji, będzie zależała od okoliczności.

Na przykład, bardziej ogólnie może być opisany zbiór *ad hoc* odnoszący się do śledztwa w toku.

83. Osoba fizyczna winna przede wszystkim mieć możliwość ubiegania się o dostęp do zbioru policyjnego bezpośrednio u administratora zbioru. Ostatecznie prawo to może być egzekwowane przez pośrednika w postaci organu nadzorczego. Prawo krajowe winno określać właściwe sposoby realizacji tego prawa. Ponadto, punkt 6.2. stanowi próbę zagwarantowania podmiotowi danych dostępu do zbioru w odpowiednim okresie czasu i bez nadmiernej zwłoki.

84. W zasadzie, żądania dostępu do danych nie powinny być rejestrowane jako, że ich rejestracja może ograniczyć egzekwowanie tego prawa. Jednakże w sytuacji, gdy Państwo Członkowskie stosuje system rejestracji, musi zadbać o to, aby rejestr wniosków był przechowywany odrębnie od przechowywanych przez Policję zwykłych zbiorów danych o sprawach karnych. Należy również rozważyć kwestię niszczenia rejestru po upływie przewidzianego prawem okresu jego przechowywania.

85. Gdy w rezultacie egzekwowania prawa dostępu wykazano niedokładność danych lub gdy ustalono, że dane są niedokładne, bez związku lub nadmierne ilościowo w wyniku zastosowania innego przepisu, punkt 6.3. stanowi, iż Policja powinna zagwarantować uporządkowanie zbioru danych. Można tego dokonać poprzez usunięcie danych niedokładnych lub skorygowanie informacji tak, aby korespondowała ze stanem faktyczym.

Jako alternatywę usunięcia, punkt 6.3. umożliwia pozostawienie danych w zbiorze, ale gdy staną się one przedmiotem dodatkowego oświadczenia wyjaśniającego prawdziwy stan rzeczy. Może tak być w sytuacji, na przykład, zeznań świadków, które okazały się być niedokładne. Zamiast całkowicie usuwać ich oświadczenia ze zbioru, pozostawienie ich może okazać się korzystne, o ile jednocześnie zostanie dołączona do nich prawdziwa wersja wydarzeń.

86. Drugi podpunkt punktu 6.3. określa harmonogram usuwania danych oraz podejmowanych środków korygujących. Należy podkreślić, iż powyższe środki zapobiegawcze nie ograniczają się jedynie do zbioru, ale muszą, w miarę możliwości, być stosowane wobec każdego innego dokumentu powiązanego ze zbiorem.

87. Doświadczenie przynajmniej jednego z Państw Członkowskich pokazało, że w zasadzie należy w większości przypadków zezwalać na dostęp do danych. Punkt 6.4. przewiduje, iż w określonych przypadkach można odmówić prawa dostępu (a wobec tego również prawa do sprostowania i usunięcia danych).

88. Należy podkreślić, że restrykcje na korzyść podmiotu danych lub praw i wolności innych osób zostały przejęte z Artykułu 9 punkt 2.b. Konwencji o Ochronie Danych. W odniesieniu do sektora Policji na stwierdzenie to składają się kwestie związane z ochroną świadków i informatorów.

89. W odniesieniu do uzasadnienia ograniczania dostępu – „niezbędnego dla wykonywania zgodnych z prawem zadań Policji" – nie ma dokładnego odpowiednika w Artykule 9 Konwencji o Ochronie Danych. Jednakże, istnieje pogląd, iż w kontekście ograniczeń prawa dostępu, derogacja Konwencji w celu „zwalczania przestępstw" jest najlepiej interpretowana właśnie w ten sposób.

90. Na jednostkę może być wywierana presja, na przykład przez przyszłego pracodawcę, aby zmusić ją do uzyskania wyciągu z kartoteki Policji. Tymczasem może nie być w interesie tej osoby pozyskiwanie pisemnej kopii czy oświadczenia o zawartości policyjnego zbioru na jej temat. W takim przypadku, prawo krajowe może zezwolić na ustne przekazanie informacji o zawartości zbioru.

91. Punkty 6.5. i 6.6. określają pewne proceduralne gwarancje na wypadek odmowy lub ograniczenia prawa dostępu, sprostowania lub usunięcia danych. Przede wszystkim odmowa lub ograniczenie musi być pisemnie umotywowane. Istotne jest wykazanie, że został spełniony obowiązek nałożony na Policję przez punkt 6.4. – dokonania oceny wagi praw podmiotu danych w odniesieniu do wspomnianych tu nadrzędnych interesów.

92. Należy podkreślić, że można odstąpić od podania przyczyn odmowy jedynie z tych samych powodów, które uzasadniają odmowę lub ograniczenie prawa dostępu, sprostowania i usunięcia. Podmiot danych winien być poinformowany o przynależnym mu prawie do odwołania się od udzielonej odmowy dostępu do danych. Prawo to winno się opierać na umotywowanej decyzji, jaka jest przewidziana w punkcie 6.5. Nawet jeśli nie podano żadnych przyczyn odmowy dostępu, ponieważ w opinii Policji w grę wchodzi interes nadrzędny, jednostkę należy poinformować o sposobie odwołania się od tej decyzji.

93. Punkt 6.6. został przygotowany w taki sposób, aby uwzględniał różnorodność praktyk w różnych Państwach Członkowskich odnośnie egzekwowania prawa dostępu. W niektórych krajach może zaistnieć sytuacja, iż osoba fizyczna nie uzyska bezpośredniego prawa

dostępu do zbioru policyjnego i będzie zobowiązana do skorzystania z pośrednictwa organu nadzorczego.

94. Nawiązanie do „innego niezależnego organu” oznacza, że w niektórych krajach dla celów odwoławczych sąd lub trybunał może zastąpić organ nadzorczy. Bez względu na taką możliwość podmiot danych, któremu odmówiono dostępu, będzie oczywiście posiadał prawo odwołania się do sądu lub trybunału w poszukiwaniu możliwości sprostowania, uzupełnienia zbioru, itd.

95. Prawo krajowe będzie określało interwencyjne kompetencje organu nadzorczego lub innego niezależnego organu odnośnie kontroli zakwestionowanego zbioru policyjnego. Może zaistnieć sytuacja, w której organ dokonujący inspekcji nie jest zobowiązany do rzeczywistego przekazywania danych jednostce nawet, gdy nie ma uzasadnienia dla odmowy dostępu. Osoba, której dane dotyczą może być po prostu poinformowana, że miała miejsce weryfikacja zbioru policyjnego, i że zbiór ten jest już uporządkowany. Ewentualnie, organ dokonujący inspekcji może zdecydować o ujawnieniu danych zawartych w zbiorze osobie, której dane dotyczą.

Zasada 7 - Okres przechowywania oraz aktualizacja danych

96. Istotne jest, aby dokonywano okresowych przeglądów zbiorów policyjnych w celu upewnienia się, że zostały oczyszczone ze zbytecznych lub niedokładnych danych oraz, że zostały zaktualizowane. Punkt 7.1. wymienia pewne okoliczności, które należy wziąć pod uwagę przy rozważaniu, czy dane są nadal niezbędne dla celów prewencji i zwalczania przestępstw oraz utrzymania porządku publicznego.

97. Punkt 7.2. wyraża życzenie autorów Rekomendacji, aby jakość danych była regularnie sprawdzana zgodnie z ustalonymi przepisami, oraz aby dane były przedmiotem ustaleń określających z mocy prawa okres ich przechowywania. Realizacja tego przepisu ułatwiłaby wykonywanie zadań, jakie nakłada na Policję podpunkt 5.5.ii. Zasady 5.

98. Prawo krajowe może zezwalać na formułowanie takich zasad. Ewentualnie zasady te mogą być formułowane przez organ nadzorczy po konsultacji z organami Policji. W przypadku, gdy Policja samodzielnie opracowuje zasady, powinna skonsultować się z organem nadzorczym co do ich treści i zastosowania.

99. Przyjmuje się, że dane policyjne są danymi o istotnej wartości dla celów statystycznych i badawczych. Krajowe ustawy o archiwach będą źródłem informacji na temat sposobów radzenia sobie z każdym problemem, jaki wyniknie w tym kontekście. O ile będzie to stosowne, należy odnieść się również do postanowień Rekomendacji R(83)10 o ochronie danych osobowych wykorzystywanych do badań naukowych i statystyki.

Zasada 8 – Zabezpieczanie danych

100. Zasada 8 odzwierciedla wymagania związane zarówno z bezpieczeństwem fizycznym, jak i poufnością. Organ odpowiedzialny, o którym wspomniano wcześniej, winien gwarantować dostęp do terminali jedynie upoważnionemu personelowi, a przekazywanie danych powinno być dozwolone stosownie do wniosków składanych zgodnie z Zasadą 5. W tym też celu organ odpowiedzialny mógłby prawdopodobnie przechowywać zapis rejestrujący informacje, o których mowa w treści punktu 5.5.i.