REKOMENDACJA R (2002)9
KOMITETU MINISTRÓW DLA PAŃSTW CZŁONKOWSKICH W SPRAWIE OCHRONY DANYCH OSOBOWYCH GROMADZONYCH I PRZETWARZANYCH DLA CELÓW UBEZPIECZENIOWYCH

(przyjęta przez Komitet Ministrów 18 września 2002 r. podczas 808 spotkania Ministrów Delegatów)

Preambuła

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

1. Zważywszy, że celem Rady Europy jest urzeczywistnienie jak najściślejszego związku między jej Państwami Członkowskimi;

2. Uwzględniając ogólne zasady dotyczące ochrony danych zawarte w Konwencji o ochronie osób w zakresie zautomatyzowanego przetwarzania danych osobowych (STE nr 108), a w szczególności jej artykuł 6, który stanowi, że dane osobowe uznane za dane szczególnie chronione nie mogą być przetwarzane, o ile prawo krajowe nie przewiduje odpowiednich gwarancji;

3. Świadomy faktu, że zautomatyzowane przetwarzanie danych osobowych dla celów ubezpieczeniowych jest coraz bardziej rozpowszechnione nie tylko dla celów przygotowywania, zawierania, wprowadzania i rozwiązywania ubezpieczenia, lecz również dla racjonalnego i ekonomicznego zarządzania ubezpieczeniami oraz dla walki z oszustwami;

4. Świadomy faktu, że ubezpieczenia świadczone są przez różne podmioty gospodarcze, w szczególności przez towarzystwa ubezpieczeniowe;

5. Przekonany o znaczeniu, jakie jakość, nienaruszalność i dostępność danych osobowych ma dla osób ubezpieczonych;

6. Zauważając, że prawie wszyscy mieszkańcy Państw Członkowskich są objęci jednym lub wieloma ubezpieczeniami, a z tego względu podmioty zajmujące się ubezpieczeniami są w posiadaniu znaczącej ilości danych osobowych, w tym również danych szczególnie chronionych;

7. Przekonany, że pożądane jest uregulowanie gromadzenia i przetwarzania danych osobowych dla celów ubezpieczeniowych, zagwarantowanie poufności i bezpieczeństwa danych oraz czuwanie nad tym, aby posługiwanie się nimi odbywało się z poszanowaniem praw i podstawowych wolności osób, w szczególności prawa do prywatności;

8. Uwzględniając fakt, że mobilność osób i globalizacja rynków oraz działalności handlowych wymagają transgranicznej wymiany informacji również w sektorze

ubezpieczeń oraz równoważnej ochrony danych we wszystkich Państwach Członkowskich Rady Europy,

Zaleca rządom Państw Członkowskich:

1. podjęcie kroków w celu odzwierciedlenia zasad zawartych w załączniku do niniejszej rekomendacji w ich ustawodawstwie i stosowanych praktykach;

2. zapewnienie szerokiego rozpowszechnienia zasad zawartych w załączniku do niniejszej rekomendacji wśród osób, instytucji i organów administracji publicznej oraz instytucji prywatnych gromadzących i przetwarzających dane osobowe dla celów ubezpieczeniowych, jak również wśród organów właściwych do spraw ochrony danych;

3. promowanie przyjęcia oraz wdrażania zasad i wytycznych znajdujących się w załączniku do niniejszej rekomendacji, w szczególności poprzez przyjęcie rozwiązań prawnych lub zachęcanie do opracowywania kodeksów etyki.

Załącznik do Rekomendacji R (2002)9

1. Definicje

W rozumieniu niniejszej rekomendacji:

a. Określenie "dane osobowe" oznacza wszelkie informacje dotyczące osoby zidentyfikowanej lub możliwej do zidentyfikowania (osoba, której dane dotyczą). Osoby fizycznej nie uważa się za „możliwą do zidentyfikowania", jeśli tego rodzaju identyfikacja wymaga nadmiernego zaangażowania czasu, sił i środków.

b. Określenie “dane szczególnie chronione” obejmuje dane osobowe ujawniające pochodzenie rasowe, poglądy polityczne, przekonania religijne lub inne przekonania, jak również dane osobowe dotyczące stanu zdrowia i życia seksualnego. Za dane szczególnie chronione uważane są również dane dotyczące prowadzonych dochodzeń i skazań, podobnie jak inne dane określone jako szczególnie chronione prawem krajowym.

c. Określenie “dla celów ubezpieczeniowych” dotyczy wszelkich operacji gromadzenia i przetwarzania danych osobowych związane z objęciem ubezpieczeniem od ryzyka, w szczególności na podstawie umowy lub polisy ubezpieczenia.

d. Określenie “przetwarzanie” oznacza każdą operację albo całość operacji prowadzonych częściowo lub całkowicie za pomocą zautomatyzowanych procesów obejmujących dane osobowe, takich jak rejestrowanie, przechowywanie lub modyfikowanie, pobieranie, przeglądanie, używanie, udostępnianie, łączenie, jak również usuwanie i niszczenie.

e. Termin “udostępnianie” oznacza umożliwienie dostępu osobom trzecim do danych osobowych, niezależnie od użytych środków lub nośników.

f. Określenie “administrator zbioru” obejmuje osobę fizyczną lub prawną, organ administracji publicznej, instytucję usługową lub wszelki inny podmiot, który, sam lub we współpracy z innymi określa cele i środki gromadzenia i przetwarzania danych osobowych.

g. Określenie “podwykonawca” oznacza osobę fizyczną lub prawną, organ administracji publicznej, instytucję usługową lub wszelki inny podmiot przetwarzający dane osobowe na rzecz administratora zbioru.

2. Zakres stosowania

2.1. Niniejsza rekomendacja ma zastosowanie do danych osobowych gromadzonych i przetwarzanych dla celów ubezpieczeniowych. Nie ma ona zastosowania do gromadzenia i przetwarzania danych osobowych dla celów zabezpieczeń społecznych.

2.2. Zachęca się Państwa Członkowskie do rozszerzenia zakresu stosowania niniejszej rekomendacji do zbiorów danych osobowych przetwarzanych w sposób niezautomatyzowany dla celów ubezpieczeniowych.

2.3. Przetwarzanie danych osobowych nie powinno być prowadzone w sposób niezautomatyzowany w celu uniknięcia stosowania postanowień niniejszej rekomendacji.

2.4. Państwa Członkowskie mogą rozszerzyć zasady, o których mowa w niniejszej rekomendacji również na gromadzenie i przetwarzanie danych dotyczących stowarzyszeń, zrzeszeń, fundacji, towarzystw, korporacji lub wszelkich innych instytucji zrzeszających bezpośrednio lub pośrednio osoby fizyczne, posiadających lub nie osobowość prawną.

2.5. Państwa Członkowskie mogą rozszerzyć stosowanie zasad niniejszej rekomendacji na ochronę danych osobowych używanych dla celów zabezpieczeń społecznych.

3. Poszanowanie prywatności

3.1. Poszanowanie praw i podstawowych wolności, a zwłaszcza prawa do prywatności, musi być zagwarantowane w czasie gromadzenia i przetwarzania danych osobowych do celów ubezpieczeniowych.

3.2. Prawo i praktyka krajowa muszą podporządkować regułom poufności osoby, które przy okazji czynności związanych z ubezpieczeniem zapoznają się z danymi osobowymi. Ponadto gromadzenie i przetwarzanie danych dotyczących stanu zdrowia powinno być prowadzone przez osoby zajmujące się zawodowo ochroną zdrowia lub przez osoby objęte regułami tajemnicy zawodowej porównywalnymi z regułami tajemnicy lekarskiej, bądź z zachowaniem gwarancji o takiej samej skuteczności, przewidzianej prawem krajowym.

4. Gromadzenie i przetwarzanie danych osobowych dla celów ubezpieczenia

Podstawowe warunki gromadzenia i przetwarzania danych osobowych

4.1. Gromadzenie i przetwarzanie (włącznie z udostępnianiem) danych osobowych powinno być prowadzone w sposób rzetelny i zgodny z prawem, dla określonych i zgodnych z prawem celów.

Dane osobowe powinny być:

- odpowiednie, istotne i niezbyt obszerne w stosunku do celów, dla których zostały zgromadzone i dla których mają być dalej przetwarzane;

- dokładne i, o ile to konieczne, uaktualnione.

Źródła danych osobowych

4.2. Dane osobowe gromadzone i przetwarzane dla celów ubezpieczenia powinny być pozyskiwane, w zasadzie, od osoby, której dotyczą lub od jej przedstawiciela prawnego.

Zgodność z prawem

4.3. Dane osobowe mogą być gromadzone i przetwarzane dla celów ubezpieczeniowych:

a. jeżeli jest to przewidziane prawem;

b. dla wykonania umowy ubezpieczenia, której osoba, której dane dotyczą jest stroną, jak również dla przygotowania takiej umowy na wniosek osoby, której dane dotyczą;

c. jeżeli osoba, której dane dotyczą lub jej przedstawiciel prawny lub organ czy osoba lub instytucja wyznaczona prawem wyraziła na to zgodę, zgodnie z Rozdziałem 6; lub

d. jeżeli dane są konieczne do realizacji uprawnionych interesów administratora zbioru, pod warunkiem, że interes osoby, której dane dotyczą nie przewyższa tego interesu.

Cel

4.4. Z zastrzeżeniem postanowień dotyczących Zasad od 4.6 do 4.8, 8.1 i 13.1, dane osobowe powinny być gromadzone i przetwarzane tyko dla celów:

a. przygotowania i udzielenia ubezpieczenia;
b. naliczania premii i fakturowania;
c. rozpatrywania wniosków o odszkodowanie i inne świadczenia;
d. reasekuracji;
e. koasekuracji;
f. zapobiegania, wykrywania i/lub ścigania oszustw ubezpieczeniowych;
g. stwierdzania, wykonywania lub obrony praw;
h. spełnienia innego szczególnego zobowiązania prawnego lub umownego;
i. poszukiwania nowych rynków ubezpieczeniowych;
j. zarządzania wewnętrznego;
k. kalkulacji ubezpieczenia.

Dane te nie mogą być dalej przetwarzane dla celów niezgodnych z pierwotnym celem, dla którego zostały zgromadzone.

Dziecko nienarodzone

4.5. Dane osobowe dotyczące dziecka nienarodzonego powinny być objęte ochroną porównywalną z ochroną danych osobowych nieletniego.

O ile prawo krajowe nie stanowi inaczej, osoba posiadająca władzę rodzicielską może występować jako osoba uprawniona do reprezentowania dziecka nienarodzonego jako osoba, której dane dotyczą.

Dane szczególnie chronione

4.6. Gromadzenie i przetwarzanie danych szczególnie chronionych powinno być zabronione, z wyjątkiem celów, o których mowa w Zasadach 4.4, 4.8, 8.1 i 13.1:

a. jeżeli osoba, której dane dotyczą lub jej przedstawiciel prawny lub inny organ czy osoba wyznaczona prawem wyraziła na to jednoznaczną zgodę, zgodnie z Rozdziałem 6; lub

b. jeżeli zezwala na to prawo oraz

i. z zastrzeżeniem odpowiednich gwarancji, jeżeli przetwarzanie jest konieczne dla celów spełnienia innego szczególnego zobowiązania prawnego lub umownego administratora danych; lub

ii. jeżeli przetwarzanie jest konieczne dla stwierdzenia, zrealizowania lub obrony prawa; lub

iii. jeżeli przetwarzanie jest konieczne dla obrony żywotnych interesów osoby, której dane dotyczą lub innej osoby w przypadku, gdy osoba, której dane dotyczą jest niezdolna fizycznie lub prawnie do wyrażenia zgody;

c. jeżeli, z zastrzeżeniem zapewnienia odpowiednich gwarancji, gromadzenie i przetwarzanie są przewidziane, dla celów ważnego interesu publicznego, bądź przez prawo bądź z mocy decyzji organu, o którym mowa w Zasadzie 15.1.

Dane dotyczące przestępstw

4.7. W derogacji Zasady 4.6, gromadzenie i przetwarzanie danych osobowych dotyczących przestępstw i karalności może być prowadzone dla celów ubezpieczeniowych pod warunkiem, że prawo krajowe zapewni odpowiednie i szczególne gwarancje oraz gdy dane te są konieczne dla walki z oszustwami ubezpieczeniowymi, dla udzielenia ubezpieczenia, dla wypłaty odszkodowania lub dla jakiegokolwiek innego świadczenia.

Marketing bezpośredni

4.8. Jeżeli osoba, której dane dotyczą została o ich przetwarzaniu poinformowana i nie wyraziła sprzeciwu, administrator danych może używać, dla celów reklamowania i promowania posiadanej gamy usług, danych zgromadzonych i zarejestrowanych dla celów ubezpieczeniowych. Jednakże, jeżeli przetwarzanie dotyczy danych szczególnie chronionych, wymagana jest jednoznaczna zgoda osoby, której dane dotyczą, o ile nie sprzeciwia się temu prawo krajowe.

Osoba, której dane dotyczą powinna być poinformowana o tym, że jej brak zgody lub jej sprzeciw w sprawie używania dotyczących jej danych osobowych dla celów marketingu bezpośredniego nie będzie zagrażało decyzji udzielenia ubezpieczenia lub korzystania z już przyznanego ubezpieczenia.

5. Informowanie osoby, której dane dotyczą

5.1. Osoby, których dane dotyczą powinny być informowane o:

a. celu lub celach, dla których dane są lub będą przetwarzane ;

b. tożsamości administratora zbioru;

c. wszelkich innych informacjach, jeżeli jest to konieczne dla zapewnienia zgodności z prawem gromadzenia danych, takich jak:

- kategorie danych, które są lub będą gromadzone;

- kategorie osób lub organów, którym dane mogą być udostępniane oraz cele tego udostępnienia;

- umożliwienie, w razie takiej potrzeby, osobom, których dane dotyczą, odmówienia zgody, wycofania zgody oraz konsekwencje takiego wycofania;

- warunki realizacji prawa dostępu i prawa sprostowania;

- osoby lub organy, od których dane są lub będą pozyskiwane;

- obowiązkowy lub fakultatywny charakter odpowiedzi na pytania będące przedmiotem gromadzenia oraz konsekwencje w stosunku do osób w przypadku nieudzielenia odpowiedzi.

5.2. Jeżeli dane pozyskiwane są bezpośrednio od osoby, której dotyczą, administrator zbioru udziela tej osobie, najpóźniej w momencie pozyskiwania danych, informacji, o których mowa w Zasadzie 5.1., o ile nie otrzymała ona tych informacji wcześniej.

5.3. Jeżeli dane nie są pozyskiwane bezpośrednio od osoby, której dotyczą, powinna ona otrzymać od administratora zbioru informacje, o których mowa w Zasadzie 5.1, w momencie rejestrowania danych lub, jeżeli przewidziane jest udostępnianie danych osobom trzecim, najpóźniej przy pierwszym udostępnieniu danych.

Obowiązek informowania osoby, której dane dotyczą nie ma zastosowania w przypadku, gdy:

a. osoba, której dane dotyczą została już poinformowana;

b. udzielenie informacji okazuje się niemożliwe lub wymagałoby nieproporcjonalnych wysiłków;

c. przetwarzanie lub udostępnianie danych dla celów ubezpieczeniowych jest jednoznacznie dozwolone prawem krajowym.

W przypadkach, o których mowa w punktach *b* i *c* przewidziane są odpowiednie gwarancje.

5.4. Informacja przeznaczona dla osoby, której dane dotyczą musi być odpowiednia i dostosowana do okoliczności.

5.5. W przypadku, gdy osoby, których dane dotyczą nie posiadają zdolności do czynności prawnych i nie są w stanie wyrażać swojej swobodnej woli oraz jeżeli prawo krajowe nie zezwala im na działanie we własnym imieniu, informacja musi być

udzielona osobie uprawnionej do występowania w imieniu osób, których dane dotyczą.

5.6. Informacja dla osób, których dane dotyczą może być ograniczona, jeżeli jest to przewidziane prawem i stanowi środek konieczny dla zapobiegania, wyjaśniania i ścigania przestępstwa lub dla zachowania praw i wolności innych osób.

6. Zgoda

6.1. W przypadku, gdy wymagana jest zgoda osoby, której dane dotyczą, musi ona być swobodna, konkretna i świadoma. Ponadto musi być niebudząca wątpliwości, a w przypadku danych szczególnie chronionych, jednoznaczna.

Jednakże mogą zaistnieć przypadki, w których prawo krajowe nie pozwala, aby zgoda była dostateczną przesłanką legalności gromadzenia lub przetwarzania danych.

6.2. W przypadku, gdy dane osobowe dotyczą osób nieposiadających zdolności do czynności prawnych i w których prawo krajowe nie zezwala osobie, której dane dotyczą występować we własnym imieniu, wymagana jest zgoda przedstawiciela prawnego lub organu lub osoby bądź instytucji określonej prawem.

6.3. Zgodnie z Zasadą 5.5. życzenie osób niezdolnych do czynności prawnych, które zostały poinformowane o zamiarze gromadzenia i przetwarzania dotyczących ich danych powinno być brane pod uwagę, o ile prawo krajowe nie stanowi inaczej.

7. Gromadzenie i przetwarzanie przez podwykonawców

7.1 Zgodnie z postanowieniami prawa krajowego administratorzy zbiorów mogą zlecić gromadzenie i przetwarzanie danych osobowych dla określonych celów, o ile są oni uprawnieni do gromadzenia i przetwarzania tych danych oraz o ile podwykonawca zobowiązuje się do działania wyłącznie według instrukcji administratora zbioru i do przestrzegania postanowień prawa krajowego wprowadzających Rozdział 11 załącznika do rekomendacji.

7.2. Administratorzy zbiorów powinni wybierać podwykonawców zapewniających wystarczające gwarancje pod względem środków technicznych i organizacyjnych. Muszą upewnić się, że środki te będą stosowane, a w szczególności, że przetwarzanie będzie prowadzone zgodnie z ich instrukcjami.

7.3. Gromadzenie i przetwarzanie danych osobowych w systemie podwykonawstwa powinno być regulowane umową lub aktem prawnym wiążącym podwykonawcę z administratorem danych, uwzględniającym w szczególności, że podwykonawca działa wyłącznie w ramach uprawnień udzielonych mu przez administratora zbioru i przez postanowienia prawa krajowego dotyczącego obowiązków podwykonawcy.

8. Udostępnianie danych do innych celów

8.1.Udostępnianie danych osobowych do celów innych niż te, o których mowa w Zasadzie 4.4 jest dozwolone tylko w przypadkach, gdzie:

a. udostępnienie jest przewidziane prawem i stanowi środek konieczny w społeczeństwie demokratycznym do zapobiegania, ścigania i karania przestępstw lub dla obrony innego ważnego interesu publicznego; lub

b. osoby, których dane dotyczą lub ich przedstawiciele prawni lub inny organ lub osoba albo instytucja wyznaczona prawem wyrazili na to zgodę, zgodnie z Rozdziałem 6; lub

c. dane udostępniane są dla celów reklamowych, o ile osoba, której dane dotyczą została o tym poinformowana i nie wyraziła sprzeciwu. Jednakże, w przypadku, gdy udostępnienie dotyczy danych szczególnie chronionych, konieczna jest wyraźna zgoda osoby, której dane dotyczą, zgodnie z Rozdziałem 6; lub

d. dane te są niezbędne dla realizacji uprawnionego celu administratora zbioru, pod warunkiem, że interes osoby, której dane dotyczą nie jest przeważający. Jednakże, jeżeli udostępnienie dotyczy danych szczególnie chronionych, zgodnie z Rozdziałem 6, byłaby konieczna wyraźna zgoda osoby, której dane dotyczą.

9. Zautomatyzowane decyzje indywidualne

9.1. Decyzje o ubezpieczeniu powodujące skutki prawne wobec osób, których dane dotyczą lub dotykające ich w znaczący sposób nie powinny być podejmowane wyłącznie na podstawie zautomatyzowanego przetwarzania danych, przeznaczonego do dokonania oceny niektórych aspektów odnoszących się do osób, których dane dotyczą na podstawie wcześniej ustalonych kryteriów lub danych statystycznych.

9.2. Decyzje takie mogą jednakże być podjęte o ile spełniają wniosek złożony przez osobę, której dane dotyczą w celu zawarcia lub wykonania umowy ubezpieczenia lub jeżeli osoba, której dane dotyczą mają możliwość przedstawienia swojego punktu widzenia w celu zagwarantowania ich uprawnionych interesów. Takie decyzje mogą również być podejmowane, jeżeli zezwala na to prawo określające środki, jakie muszą być podjęte w celu zagwarantowania zabezpieczenia uprawnionych interesów osoby, której dane dotyczą.

10. Prawo dostępu i prawo sprostowania

10.1. Każda osoba, która złoży o to wniosek, powinna otrzymać potwierdzenie faktu, czy dotyczące jej dane są przetwarzane czy nie, jak również otrzymać wszystkie informacje w formie zrozumiałej, dotyczące celu przetwarzania, kategorii danych podlegających przetwarzaniu, odbiorców lub kategorii odbiorców, którym dane zostały udostępnione oraz pochodzenie danych. Powinny również zostać poinformowane o systemie logicznym, według którego odbywa się zautomatyzowane przetwarzanie dotyczących ich danych, przynajmniej w przypadku zautomatyzowanych decyzji indywidualnych.

10.2. Prawa osób, których dane dotyczą do otrzymywania dotyczących ich danych nie powinny być ograniczone o ile nie jest to przewidziane prawem i nie jest konieczne do:

a. zapobiegania, ścigania lub karania przestępstw;

b. ochrony praw i wolności osób, których dane dotyczą lub innych osób.

W takich przypadkach prawo dostępu może być ograniczone przez okres trwania przyczyn tego ograniczenia.

10.3. Osoby, których dane dotyczą powinny uzyskać, w zależności od przypadku, sprostowanie, usunięcie lub zablokowanie dotyczących ich danych, jeżeli zostały one zgromadzone lub były przetwarzane z pominięciem postanowień prawa krajowego wprowadzającego zasady zawarte w niniejszej rekomendacji, w szczególności, gdy dane te okażą się niedokładne, nieistotne lub zbyt obszerne.

10.4. Powody ograniczenia prawa dostępu, sprostowania, usunięcia lub zablokowania powinny zostać podane w formie pisemnej. W przypadku ograniczenia dostępu osobie, której dane dotyczą, jak również ograniczenia jej prawa do sprostowania, usunięcia lub zablokowania danych, osoba ta powinna być poinformowana o przysługującym jej prawie do zwrócenia się do właściwego organu z wnioskiem o sprawdzenie zgodności z prawem przetwarzania.

10.5. Osoby trzecie, którym dane zostały udostępnione powinny być poinformowane o dokonanym sprostowaniu, usunięciu lub zablokowaniu, o ile nie okaże się to wyraźnie nieracjonalne lub niewykonalne.

10.6. Administrator zbioru powinien, w rozsądnych odstępach czasu oraz bez nadmiernej zwłoki i kosztów udostępniać dane osobowe osobie posiadającej do nich prawo dostępu, jak również wszelkie informacje, o których mowa w Zasadzie 10.1, wobec których realizowane jest prawo dostępu.

11. Bezpieczeństwo danych

11.1. Należy wprowadzić odpowiednie środki techniczne i organizacyjne dla zapewnienia ochrony danych osobowych przetwarzanych zgodnie z postanowieniami prawa krajowego wprowadzającego zasady zawarte w niniejszej rekomendacji, przed zniszczeniem – przypadkowym lub celowym - oraz przed przypadkową utratą i nieuprawnionym dostępem, zmianą lub udostępnieniem i przed wszelkimi innymi formami nielegalnego przetwarzania.

Środki te powinny zapewniać odpowiednią ochronę z uwzględnieniem z jednej strony możliwości technicznych a z drugiej strony szczególnego charakteru danych gromadzonych i przetwarzanych dla celów ubezpieczeniowych oraz oceny potencjalnych zagrożeń. Powinny one podlegać okresowej analizie.

11.2. W celu zapewnienia zwłaszcza poufności, nienaruszalności i dostępności przetwarzanych danych, jak również dla ochrony osób, których dane dotyczą, administrator zbioru powinien podjąć odpowiednie kroki w celu:

a. uniemożliwienia dostępu wszelkim nieuprawnionym osobom do urządzeń używanych do przetwarzania danych osobowych (kontrola dostępu do urządzeń);

b. zabezpieczenia nośników danych przed odczytaniem, skopiowaniem, zmianą lub przemieszczeniem przez osobę nieuprawnioną (kontrola nośników danych);

c. uniemożliwienia nieuprawnionego wprowadzenia danych do systemu informatycznego, jak również jakiegokolwiek nieuprawnionego zapoznania się, modyfikacji lub usunięcia zarejestrowanych danych osobowych (kontrola pamięci);

d. uniemożliwienia użycia przez osoby nieuprawnione zautomatyzowanych systemów przetwarzania danych za pomocą urządzeń do przesyłania danych (kontrola użytkowania);

e. zapewnienia, z jednej strony, ze względu na selektywny dostęp do danych a z drugiej strony ze względu na bezpieczeństwo danych osobowych, że przetwarzanie jest z zasady pomyślane w sposób umożliwiający oddzielenie:

- danych identyfikacyjnych i danych odnoszących się do tożsamości osób,
- danych administracyjnych,
- danych szczególnie chronionych (kontrola dostępu).

f. zagwarantowania możliwości sprawdzenia i stwierdzenia, jakim osobom lub jakim organom mogą być udostępniane dane osobowe za pośrednictwem urządzeń do transmisji danych (kontrola połączeń);

g. zapewnienie możliwości sprawdzenia i stwierdzenia a posteriori kto miał dostęp do systemu oraz jakie dane zostały wprowadzone do systemu informatycznego, w jakim momencie i przez kogo (kontrola wprowadzania danych);

h. zabezpieczenie w czasie udostępniania danych osobowych, jak również w czasie transportu nośników danych przed ich odczytaniem, kopiowaniem, zmianą lub usunięciem w sposób niedozwolony (kontrola transportu);

i. zabezpieczenia danych za pomocą kopii bezpieczeństwa (kontrola dostępności).

11.3. Administratorzy danych muszą, zgodnie z prawem krajowym, wprowadzić odpowiednie regulacje wewnętrzne zgodne z istotnymi zasadami zawartymi w niniejszej rekomendacji.

11.4. W razie konieczności administratorzy danych muszą wyznaczyć niezależną osobę odpowiedzialną za bezpieczeństwo systemów informatycznych i za ochronę danych, właściwą do udzielania porad w tych kwestiach.

12. Transgraniczny przepływ danych

12.1. Zasady niniejszej rekomendacji mają zastosowanie do transgranicznego przepływu danych osobowych gromadzonych i przetwarzanych dla celów ubezpieczeniowych.

12.2. Transgraniczny przepływ danych do państwa, które ratyfikowało Konwencję o ochronie osób w zakresie zautomatyzowanego przetwarzania danych osobowych (STE n° 108) i posiadającego ustawodawstwo zapewniające równoważną ochronę danych nie powinno być objęte szczególnymi warunkami ochrony prywatności.

12.3. Nie powinno być ograniczeń transgranicznego przepływu danych do państwa, które nie ratyfikowało Konwencji, lecz zapewnia odpowiednią ochronę danych.

12.4. O ile prawo krajowe nie stanowi inaczej, transgraniczny przepływ danych do państwa niezapewniającego odpowiedniego poziomu ochrony nie powinien, w zasadzie, mieć miejsca, chyba, że:

a. osoba, której dane dotyczą wyraziła na to zgodę, zgodnie z Rozdziałem 6; lub

b. zostały podjęte konieczne środki, włącznie z umownymi, mające na celu przestrzeganie prawa krajowego wprowadzającego zasady Konwencji i niniejszej rekomendacji, a osoba, której dane dotyczą miała możliwość sprzeciwienia się przekazaniu danych.

13. Przechowywanie danych

13.1. W przypadku, gdy dane nie są już potrzebne do realizacji celów, dla których zostały zgromadzone i przetworzone przez administratora danych, powinny zostać usunięte. Zasada ta ma zastosowanie również wtedy, gdy została już podjęta decyzja o odmowie ubezpieczenia. Jeżeli jednak muszą one być zachowane, dla celów badań naukowych lub dla celów statystycznych lub dla innych celów przewidzianych prawem, muszą one być przechowywane osobno, dostępne wyłącznie dla tych celów i z zastosowaniem odpowiednich gwarancji.

13.2. Odnośnie do okresu przechowywania danych uwzględniana jest zwłaszcza konieczność przechowywania danych przez okres wymagany dla działań prawnych, dla sporządzenia dowodów transakcji lub dla uzasadnienia decyzji o odmowie ubezpieczenia.

14. Odwołanie

Prawo krajowe powinno przewidywać sankcje i odpowiednie zasady odwoływania się w sprawach związanych z naruszeniem przepisów prawa krajowego wprowadzającego zasady niniejszej rekomendacji.

15. Gwarancje przestrzegania zasad

15.1. Państwa Członkowskie upoważniają jeden lub więcej organów, pełniących swoje funkcje w pełnej niezależności, do czuwania na przestrzeganiem stosowania prawa krajowego wprowadzającego zasady niniejszej rekomendacji.

15.2. Następujące informacje powinny być podane do publicznej wiadomości w odpowiedni, łatwo dostępny sposób:

a. nazwa i adres administratora zbioru oraz jego przedstawiciela, jeżeli taki istnieje;

b. cel lub cele przetwarzania;

c. kategorię lub kategorie danych oraz osób, których dane dotyczą;

d. odbiorcy lub kategorie odbiorców, którym dane mogą być udostępniane;

e. przewidywane przekazy danych do państw trzecich.