Andrzej Lewiński
Zastępca Generalnego Inspektora
Ochrony Danych Osobowych

Kodeks Dobrych Praktyk jako Gwarant Postępowań Zgodnych z Ochroną Danych Osobowych.

Przepisy stanowiące regulacje prawne dotyczące sfery ochrony danych osobowych stały się w latach 70, przedmiotem zainteresowania prawników europejskich. Pierwszą regulacją mającą wymiar ustawowy była uchwalona w 1970 r. ustawa o ochronie danych osobowych w Hesji, wyprzedzająca o kilka lat ustawę federalną w Niemczech. W Polsce należy wspomnieć, iż za sprawą cywilisty szkoły krakowskiej prof. Andrzeja Kopffa została przedstawiona teza, iż sfera życia prywatnego podzielona została na dwie „podsfery". Obejmowały one sferę intymnego życia osobistego i sferę prywatnego życia osobistego. Sfery te różniły się od siebie przede wszystkim zakresem, w jakim jednostka jest skłonna dopuszczać innych do informacji należących do danej sfery. Do sfery życia intymnego zaliczono takie przeżycia osobiste człowieka, z którymi nie dzieli się on na ogół z nikim albo tylko z najbliższą rodziną. Z tak podanego podziału na sfery wypływa zróżnicowanie intensywności ochrony. Według prof. A Kopffa żadne okoliczności nie dają podstaw na ingerencję osób trzecich w sferę intymnego życia osobistego człowieka. Można przyjąć ze tak pojęta i zdefiniowana prywatna sfera życia człowieka jest podstawą uregulowań prawnych i ich interpretacji w do dzisiaj stosowanym prawie.
Ochrona prawa do prywatności uwzględniona została w Europejskiej Konwencji Praw Człowieka z 1950 roku. W art. 8 tej Konwencji wpisano prawo do poszanowania życia prywatnego i rodzinnego.
Niewątpliwie funkcję podstawowej międzynarodowej regulacji poświeconej ochronie danych osobowych pełni Konwencja Rady Europy z dnia 28 stycznia 1982 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Celem

Konwencji było między innymi zapewnienie bezpieczeństwa poszanowania sfery osobistej.
W Konwencji zakreślone zostały podstawy późniejszych rozwiązań w ustawodawstwach krajowych. Mając na uwadze nasz dzisiejszy temat dotyczący zasad etyki czy dobrych praktyk to należy zwrócić uwagę na zapisy art. 5 i 6, w którym mówi się, iż: „Przetwarzane automatycznie dane osobowe muszą być:
a) uzyskiwane i przetwarzane w dobrej wierze i w sposób zgodny z prawem;
b) gromadzone dla oznaczonych z prawem celów i nie mogą być wykorzystywane niezgodnie z tymi celami;
c) odpowiednie oraz istotne dla celów, dla których są gromadzone i nie mogą poza te granicę wykraczać;
d) właściwe merytorycznie oraz, jeśli to konieczne, odnoszące się do najnowszego stanu;
e) przechowywane tak, ażeby osoba , której dotyczą, nie mogła być identyfikowana dłużej, niż to konieczne dla celu, dla których jest gromadzone.
Powyżej przedstawione zasady były podstawa dla odpowiednich zapisów w tym przedmiocie zapisanych w Dyrektywie 95/46 oraz Ustawie o Ochronie danych osobowych (art. 26 ustawy).

Wśród europejskich aktów, których przepisy mogą mieć wpływ na zasady etyki czy dobre praktyki to należałoby wymienić również dwie Rezolucje Komitetu Ministrów Rady Europy uchwalonych w 1973 i 1974 roku. Dotyczą one ochrony prywatności osób fizycznych przy wykorzystywaniu elektronicznych banków danych. (rezolucje 22 i 29). W rezolucji numer 22 chciałbym zwrócić uwagę na następujące zasady:

a) gromadzone informacje powinny być dokładne i aktualne przy czym w zasadzie nie powinny to być informacje dotyczące „ścisłego” życia prywatnego lub takie, które mogłyby łatwo prowadzić do dyskryminacji, a gdy tego rodzaju informacje są już zbierane – nie powinny być rozpowszechniane;
b) informacje nie powinny być uzyskiwane sposobami podstępnymi lub nieuczciwymi;
c) należy zastosować środki ostrożności zapobiegające niewłaściwemu lub podstępnemu wykorzystywaniu informacji;

d) dane statystyczne powinny być dostępne tylko w formie zbiorczej i w sposób, który uniemożliwiłby łączenie tych informacji z określonymi osobami.

W Rezolucji 29 powtórzony został zapis, iż: **„Dane wykorzystywane dla celów statystycznych mogą być rozpowszechniane tylko w sposób uniemożliwiający powiązanie ich z oznaczonymi osobami”.** W dwóch nowych Rezolucjach, w stosunku do poprzedniej rezolucji, zwrócono uwagę na zakładanie w sektorze publicznym banków danych oraz wskazano warunki, jakie musza być spełnione, gdy przedmiot przetwarzania dotyczy danych należących do sfery intymnej osób fizycznych.

W zasadniczy sposób do kwestii zasad etyki czy dobrych praktyk odniesiono się w Dyrektywie 95/46 WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. W Rozdziale V nazwanym Kodeksy Postępowania w art. 27 zapisano szereg przepisów regulujących tę kwestię. Państwa członkowskie i Komisja zostały zobowiązane do zachęcania do opracowywania kodeksów postępowań, których celem będzie usprawnienie procesu prawidłowego stosowania krajowych przepisów ochrony danych osobowych, uwzględniając specyficzne cechy różnych branż. Państwa członkowskie zostały zobowiązane do umożliwienia stowarzyszeniom zawodowym i innym instytucjom reprezentującym inne kategorie administratorów danych wypracowania kodeksów postępowania oraz dokonania oceny ich zgodności z prawem krajowym.

Przewiduje się możliwość wypracowania kodeksów Wspólnoty, które mogą być przedstawione do zaopiniowania zespołowi roboczemu działającemu na podstawie art. 29 Dyrektywy 95/46 WE. Komisja również może zapewnić odpowiednie rozpowszechnienie takiemu kodeksowi postępowania dotyczącemu określonej branży pod warunkiem uprzedniego zaopiniowania pozytywnego przez Zespół Roboczy art. 29 Dyrektywy.

Podstawowym przepisem prawa regulującym ochronę danych osobowych w Polsce jest Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Stanowi ona implementację przepisów Dyrektywy 95/46 WE oraz wykonanie zapisów w

Konstytucji RP. Zapisy Konstytucji RP nie obejmują wszystkich przejawów zbierania i przetwarzania danych osobowych. Zapisy dotyczą według ustawodawcy najważniejszych interesów obywatelskich. Polski system prawny przyjmuje zasadę (prawo do) samodzielnego decydowania każdej osoby o ujawnieniu dotyczących jej informacji (Komentarz J. Barta, P. Fajgielski R. Markiewicz). Ograniczeniem bezwzględnej ochrony przetwarzania danych osobowych jest zapis w art. 51 ust. 2 Konstytucji, który mówi, iż: „Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym". Również: „zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa „ (art.51 ust.5). Wzbudza różnice zdań interpretacja zapisu „niezbędne w demokratycznym państwie prawa". W Konwencji 108, której sygnatariuszem jest Polska, w art. 9 wskazano, iż możliwe są wyjątki regulacji dotyczących przetwarzania i udostępniania danych osobowych. Odstąpienia od przepisów je regulujących są dopuszczalne, jeśli przewiduje to prawo krajowe jako środek konieczny w społeczeństwie demokratycznym w dwóch przypadkach: a) ochrony państwa, interesów finansowych państwa lub dla utrzymania porządku i bezpieczeństwa publicznego oraz zwalczania przestępczości;
b) ochrony osoby , której dane dotyczą , albo praw i wolności innych osób.
Stanowi problem , jak wśród innych wolności zapisanych między innymi w Konstytucji RP znaleźć kompromisowe rozwiązania.
Wypowiedział się na ten temat Europejski Trybunał Sprawiedliwości, który w Wyroku z 6 listopada 2003 r. (sprawa C- 101/01) odniósł się do tego problemu w sposób następujący**:**
„Przepisy Dyrektywy 95/46 jako takie nie wprowadzają ograniczenia z zasadami dotyczącymi swobody wypowiedzi bądź innymi wolnościami i prawami, które znajdują zastosowanie na terenie Unii Europejskiej oraz zagwarantowane m. in. Przez art. 10 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności podpisanej w Rzymie w dniu 4 listopada 1950 r. To na władzach krajowych oraz sądach odpowiedzialnych za stosowanie prawa krajowego implementującego Dyrektywę 95/46 spoczywa obowiązek zapewnienia należytej równowagi pomiędzy wchodzącymi w grę prawami i interesami, w tym

prawami podstawowymi chronionymi przez wspólnotowy porządek prawny".

Powracając do reguł i zasad wprowadzania kodeksów postępowania, których podstawą są przepisy art. 27 Dyrektywy 95/46 grupa robocza art. 29 Dyrektywy przyjęła we wrześniu 1998 r. dokument wyjaśniający procedurę, jaką należy stosować przy przyjmowaniu wspólnotowych reguł (kodeksów postępowania) przez zainteresowane strony i przy ich późniejszej ocenie przez grupę roboczą zgodnie z art. 27 i 29 Dyrektywy 95/46 WE.
W 1998 r. Europejska Federacja Marketingu Bezpośredniego (FEDMA) przedstawiła grupie roboczej do analizy pierwszy projekt reguł. W celu dokonania analizy i zaopiniowania projektu utworzona została specjalna grupa robocza składająca się z trzech delegatów grupy tj. przedstawicieli holenderskiego, francuskiego i brytyjskiego organu ochrony danych. Grupa robocza zwróciła się również o opinię w tej sprawie do przedstawicieli zainteresowanych osób i uzgodniła z BEUC (europejska organizacja konsumentów) treść reguł. Grupa robocza uznała, iż przedstawiony przez FEDMA kodeks postępowania jest zgodny z Dyrektywą 95/46 WE i przynosi wystarczającą wartość dodaną do Dyrektywy, jako, że jest odpowiednio skupiony na kwestiach i problemach związanych z ochroną danych w sektorze marketingu bezpośredniego. Grupa robocza art. 29 podkreśliła, że kodeks ogólny nie pozwala z definicji rozwiązać całości specyficznych problemów działalności on – line, zachęca więc FEDMA do opracowania załącznika zajmującego się tymi kwestiami. Załącznik ten powinien zwłaszcza skupić się na ochronie dzieci, które są szczególnie narażone przy operacjach on – line. Grupa zwróciła się do FEDMA o aktywne promowanie tego kodeksu postępowania w środowiskach podmiotów związanych z marketingiem bezpośrednim, jak również kontynuowania prac w tej dziedzinie, w celu podniesienia poziomu ochrony danych oferowanego osobom fizycznym. Strony uzgodniły, iż FEDMA będzie składała coroczne sprawozdania ze stosowania kodeksu.

FEDMA, Europejska Federacja Marketingu Bezpośredniego opublikowała, Europejski Kodeks Deontologiczny w Sprawie

Posługiwania się Danymi Osobowymi oraz wydała Memorandum Wyjaśniające (tekst Memorandum przedstawiam jako załącznik).

Realizując wytyczne Grupy Roboczej art. 29 Generalny Inspektor Ochrony Danych w 2008 roku podpisał Porozumienie ze Stowarzyszeniem Marketingu Bezpośredniego o wspólnych działaniach na rzecz poprawy poziomu ochrony danych osobowych i prawa do prywatności w działalności marketingowej oraz stosowaniu Kodeksu Dobrych Praktyk.
Załącznikiem porozumienia był Kodeks Dobrych Praktyk Stowarzyszenia Marketingu Bezpośredniego w zakresie ochrony danych osobowych. (http://www.smb.pl/public/files/File/kodeks_etyczny_smb.pdf)
Zawarte porozumienie jest dobrym przykładem współpracy na rzecz podnoszenia poziomu ochrony danych osobowych w działalności tego niezwykle ważnego i wrażliwego na prawa obywatelskie sektora gospodarczego .

Realizując postanowienia Grupy Roboczej art.29 d.s. ochrony danych osobowych, Europejska Federacja Marketingu Bezpośredniego i Interaktywnego w czerwcu 2010 r. przedstawiła nowy dokument (uzupełniający) pod nazwą: Europejski Kodeks Postępowania w zakresie wykorzystywania danych osobowych - Aneks w zakresie komunikacji elektronicznej. Przedstawiony dokument stanowi rozszerzenie Kodeksu o nowe dziedziny związane z nowoczesnymi technologiami a szczególnie z Internetem.

Grupa Robocza art. 29 d.s. ochrony danych osobowych w lipcu 2010 r. wydała Opinię 4/2010 w sprawie Europejskiego Kodeksu Postępowania FEDMA w zakresie wykorzystywania danych osobowych w marketingu bezpośrednim - w zakresie komunikacji internetowej (tekst w załączeniu).

Generalny Inspektor Ochrony Danych Osobowych zawarł również porozumienie o współpracy ze Związkiem Banków Polskich. Efektem tego porozumienia było wypracowanie przy udziale pracowników Biura GIODO zapisów w Zasadach Dobrej Praktyki Bankowej, rozdziału obejmującego zasady przetwarzania danych osobowych.

GIODO na roboczo współpracuje z Komisją Etyki Bankowej przy Związku Banków Polskich. Jedną z form tej współpracy jest wkład, jaki wnosi GIODO w corocznie opracowywanym przez Komisję Etyki Bankowej, Raporcie, obejmującym między innymi ocenę zachowań banków w relacjach dwustronnych oraz przestrzegania zasad uczciwej konkurencji. Przedmiotem takiego badania przez Komisję Etyki Bankowej jest poziom ochrony danych osobowych w działalności banków i zgodność przetwarzania danych z przepisami o ochronie danych osobowych. Z inicjatywy wspomnianej Komisji jest wypracowywana przez GIODO opinia na temat przestrzegania przepisów o ochronie danych osobowych, na podstawie analizy skarg na działalność sektora bankowego oraz przeprowadzonych przez GIODO inspekcji. Na szczególne podkreślenie zasługuje pytanie, z jakim zwróciła się Komisja Etyki do GIODO: „Czy jakość ochrony danych osobowych wykazuje w badanym okresie poprawę, a także, jaki wpływ na ten stan rzeczy może mieć poziom szkolenia zawodowego w bankach". Wynikiem tego współdziałania, było wypracowanie przez Biuro GIODO a zaopiniowane przez Związek Banków Polskich opracowanie pod nazwą „ABC przetwarzania Danych Osobowych w sektorze bankowym" (www.giodo.gov.pl). W tym zakresie efekty współpracy można ocenić jako wielce satysfakcjonujące.

GIODO jest w trakcie wypracowywania porozumień o współpracy w zakresie między innymi kodeksów postępowań z innymi branżami czy środowiskami zawodowymi, w tym z Polskim Związkiem Przemysłu Motoryzacyjnego, Związkiem Pracodawców Firm Internetowych oraz Naczelną Izbą Lekarską. Sygnały o konieczności podjęcia takich działań otrzymuje GIODO z innych środowisk gospodarczych czy zawodowych. Należy w tym miejscu wspomnieć, iż GIODO i Polska Izba Ubezpieczeń podjęli decyzję o przystąpieniu do prac na rzecz dokumentu o współpracy wzajemnej jak i kodeksu dobrych praktyk.

Komisja Europejska opublikowała Raport pod nazwą „Pierwszy Raport NT. wdrażania Dyrektywy o ochronie danych osobowych (95/46/WE)". Przedstawiony Raport stanowi kontrolę poszczególnych aktów prawnych państw członkowskich w zakresie ochrony danych osobowych. Komisja stwierdziła, iż od roku 1995, kiedy przyjęto

Dyrektywę nastąpił ogromny rozwój i wzrost liczby użytkowników Internetu. Stwierdzono, iż wzrost zainteresowania Internetem spowodował „eksplozję danych", co nasuwa wątpliwości, czy prawo jest w stanie sobie poradzić z tego rodzaju wyzwaniem, a szczególnie tradycyjne ustawodawstwo, o ograniczonym zakresie geograficznym swego zastosowania, który nie ma znaczenia dla użytkowników poruszających się w Internecie. W toku przeprowadzonej dyskusji wyraźnym jest postulat zmiany Dyrektywy 95/46/WE. Wśród wielu projektów zmian były i takie, które dotyczyły głównie zmniejszenia ciężarów związanych z osiągnięciem działań zgodnych z przepisami o ochronie danych osobowych przez administratorów danych. **Komisja wypowiada się zdecydowanie, iż proponowane zmiany, które mogłyby być wzięte pod uwagę we właściwym czasie, powinny zmierzać do utrzymania obecnego poziomu ochrony i muszą być spójne z ogólnymi ramami zapewnionymi przez istniejące obecnie międzynarodowe instrumenty prawne. Aby podkreślić te zapowiedzi należy przytoczyć słowa Komisarza Komisji Europejskiej Frederika Bolkesteina, który podczas sesji zamykającej Konferencję na temat wdrażania Dyrektywy powiedział: „Nie możemy mówić w tym przypadku o czystej kartce papieru, gdy chodzi o tworzenie polityki ochrony danych osobowych (…). Przygotowując ten Raport Komisja będzie musiała mieć na uwadze szersze ramy polityczne i prawne, w szczególności zawarte w Konwencji 108".**

W podsumowaniu Raportu wskazano na działania należące do parytetów, według Komisji. W działaniu 9 stwierdzono, iż Komisja jest rozczarowana faktem, iż tak niewiele organizacji zgłosiło chęć stosowania Kodeksów Postępowania na poziomie Wspólnoty. Komisja zwróciła się do sektorów i grup interesów do podjęcia działań z dużym wyprzedzeniem, i wyraziła przekonanie, iż samoregulacje, a w szczególności kodeksy postępowania powinny odegrać ważna rolę, gdy chodzi o przyszłość ochrony danych we Wspólnocie i poza nią. W konkluzji Raportu, Komisja wyraziła pogląd, który może mieć istotne skutki dla stosowania i interpretacji niektórych przepisów dotyczących ochrony danych osobowych. W szczególności Komisja stwierdziła, iż: „państwa członkowskie i organy nadzorcze podejmą wszelkie odpowiednie kroki w celu

stworzenia środowiska, w którym administratorzy danych – i nie tylko ci działający na poziomie Wspólnoty czy na poziomie międzynarodowym – będą mogli dostosować się do określonych wymagań w mniej złożony i uciążliwy sposób oraz unikną nakładania na nich wymagań, które mogą być pominięte bez żadnych skutków ubocznych dla wysokiego poziomu ochrony danych zagwarantowanego w Dyrektywie".

Komisja ponadto podkreśla niezwykle istotną rolę, jaką dla ochrony danych osobowych odgrywa poziom świadomości osób, których dane są przetwarzane, a także osób i podmiotów przetwarzających dane osobowe. Komisja wskazuje, iż organy ochrony danych krajów unijnych winny przeznaczać większe ilości środków na te cele.

Rozwój nowych technologii jest wyzwaniem dla zapewnienia właściwego poziomu ochrony danych osobowych. Pojawienie się ekonomii opartej na wiedzy (informacji) wraz z postępem technologicznym i wzrastającą „potrzebą" licznych środowisk gospodarczych na zbieranie jak najwięcej danych i informacji o osobie wzbudza w Komisji Europejskiej szereg obaw o zapewnienie skutecznej ochrony danych osobowych. Sfera ubezpieczeniowa jest jednym z tych środowisk gdzie odnotowuje się takie potrzeby.

Dla przykładu można wymienić najbardziej aktualne „wydarzenie", jakim jest wprowadzanie nowej technologii systemu RFID. Identyfikacja radiowa (RFID) stanowi nowy etap rozwoju społeczeństwa informacyjnego, w którym obiekty wyposażone w mikroelektronikę, mogącą automatycznie przetwarzać dane, w coraz większym stopniu będą stawały się integralną częścią życia codziennego.

Szereg kategorii danych osobowych może być uważana za powiązana z aplikacjami RFID. Należy do nich zaliczyć następujące kategorie:

- Behawioralne;
- Biometryczne;
- Dane kontaktowe;
- Wyroki za przestępstwa kryminalne;
- Demograficzne;
- Wykształcenie i inne umiejętności;
- Dane dotyczące zatrudnienia;
- Powiązania rodzinne i inne dane socjalne;

- Finansowe;
- Genetyczne;
- Stan zdrowia;
- Kontakty osobiste;
- Zdjęcia i nagrania wideo;
- Przekonania polityczne;
- Pochodzenie rasowe i etniczne;
- Przekonania religijne;
- Życie seksualne;
- Transakcje i zakupy;
-Numery rejestracyjne pojazdu.

Te wymienione wyżej kategorie danych nie stanowią katalogu zamkniętego. Europejski Inspektor Danych Osobowych w swojej Opinii (2008/C 101/02) w sprawie Komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno – Społecznego i Komitetu Regionów w sprawie „Identyfikacji radiowej (RFID) w Europie; w stronę ram polityki „COM(2007)96, wskazał na dużą rolę, w jaką, przy wdrażania i przetwarzaniu tej technologii mogą odgrywać instrumenty samoregulacyjne. W pierwszej fazie wdrażania tego systemu uznał, podobnie jak Komisja, iż należy zostawić miejsce do samoregulacji, aby pozwolić stronom zainteresowanym szybko stworzyć warunki zgodne z prawem. Europejski Rzecznik w ust. 37 Opinii stwierdził:
„W komunikacie przewiduje się, że samoregulacja przyjmie formę kodeksu postępowania lub kodeksu dobrych praktyk. Zdaniem EIOD, niezależnie od tego, jaką formę przyjmie samoregulacja, powinna ona:
- dawać konkretne i praktyczne wskazówki na temat poszczególnych rodzajów zastosowań RFID, a co za tym idzie przyczyniać się do zgodności z ramami prawnymi w zakresie ochrony danych,
- rozwiązywać poszczególne kwestie i problemy, które pojawiają się w kontekście ogólnych zastosowań RFID,
- przyczyniać się do jednolitego i harmonijnego stosowania dyrektywy o ochronie danych w całej UE, a dokładniej w tej branży, która najprawdopodobniej będzie stosowała ten rodzaj aplikacji RFID w całej UE,

EIOD zwraca uwagę na jedno zagadnienie, w którym samoregulacja będzie szczególnie przydatna. W przypadku zastosowań RFID, które zakładają przetwarzanie danych osobowych, dyrektywa nakłada na administratora danych różne zobowiązania. Zgodnie z tymi przepisami administratorzy danych. Muszą ustanowić środki zapobiegające nieuprawnionemu ujawniania danych. Z drugiej strony administratorzy danych muszą zadbać o to, by przetwarzanie, takie jak ujawnienie informacji dzięki czytnikom – w odpowiednich przypadkach – odbywało się jedynie po uzyskaniu świadomej zgody osoby, której te dane dotyczą. Szczególnie należy podkreślić stanowisko EIOD, które mówi iż: „Chociaż EIOD jest zdania, że zasada wyrażania zgody w punkcie sprzedaży jest zobowiązaniem prawnym, które w większości przypadków wynika z dyrektywy o ochronie danych osobowych, zobowiązanie to należy wyszczególnić w instrumentach samoregulacyjnych".

Można interpretować, że te przepisy dyrektywy o ochronie danych wymagają, aby aplikacje RFID były stosowane przy zapewnieniu koniecznych rozwiązań technicznych, które będą zapobiegały lub minimalizowały ryzyko niechcianego ujawnienia danych i w odpowiednich przypadkach gwarantowały przetwarzanie danych lub dokonywały ich transferu jedynie po uzyskania świadomej zgody. Zdaniem EIOD takie zobowiązanie (tj. stosowanie koniecznych rozwiązań technicznych, które będą zapobiegały lub minimalizowały ryzyko niechcianego ujawnienia danych) i jego wiążącego charakteru dla stosujących RFID będą jeszcze bardziej zdecydowane i jasne, jeśli wymóg ten zostanie zawarty w kodeksie dobrych praktyk lub w kodeksie postępowania. Z tych powodów EIOD zdecydowanie radzi, aby zalecenia Komisji zawierało taką interpretację dyrektywy o ochronie danych, podkreślając istnienie obowiązku rozmieszczania aplikacji RFID z zastosowaniem koniecznych rozwiązań technicznych, które będą zapobiegały niechcianemu gromadzeniu lub ujawnianiu informacji".

W dniu 13 lipca 2010 roku Grupa Robocza art. 29 ds. ochrony Danych przyjęła Opinię 5/2010 w sprawie sektorowej propozycji ram dla oceny skutków aplikacji RFID w zakresie ochrony danych i

prywatności . Odnosząc się do systemu RFID i doceniając oczywiste zalety tej technologii ale stwierdzono również na potencjalne zagrożenia wynikające w szczególności z : „ możliwości wykorzystania technologii RFID przez firmy i władze w celu ingerowania w sferę prywatną obywateli „ i dalej „ możliwości potajemnego zbierania rozmaitych danych dotyczących tej samej osoby , śledzenia obywateli poruszających się w miejscach publicznych (lotniskach , dworcach , sklepach) wzbogacania profili poprzez monitorowanie zachowań konsumentów w sklepach , odczytywanie informacji o ubraniach i akcesoriach noszonych przez klientów oraz o lekach , jakie oni maja przy sobie – to przykłady wykorzystania RFID w sposób budzący obawy w zakresie prywatności : . W Opinii Grupa odnosi się również do „ samoregulacji „ jako istotnego czynnika w procesie wdrażania zasad ochrony prywatności i ochrony danych w zastosowaniach wspieranych identyfikacją radiową . Należy przypomnieć iż Komisja Europejskie w Rekomendacji dotyczącej przedmiotowego tematu wprowadziła istotna nowość to znaczy wymaganie aby operatorzy RFID przeprowadzili ocenę wpływu tych technologii na ochronę danych i prywatności . Ocena powinna być dokonana przed rozpoczęciem stosowania aplikacji RFID . Operatorzy zostali zobowiązani do udostępnienia wyników tej oceny właściwemu organowi ochrony danych osobowych na co najmniej sześć tygodni przed wdrożeniem aplikacji . Sposób jej udostępnienia winien zostać ustalony przez krajowe organy ochrony danych . W szczególności uwzględnić należy zagrożenia związane z aplikacją oraz inne czynniki , takie jak obecność administratora danych . Grupa robocza nie udzieliła poparcia dla proponowanego dokumentu przedstawionego przez ds. RFID . Tak przyjęte stanowiska , Komisji UE , EIOD czy Grupy Roboczej art. 29 daje możliwość środowiskom stosującym te nowe technologie do wykorzystania i wykazania potencjału samoregulacji jako dodatkowego , elastycznego i efektywnego narzędzia dla ram prawnych UE w świetle szybko zachodzących zmian technologicznych .

Przedmiot działalności ubezpieczeniowej w sposób bezpośredni dotyka praw konstytucyjnych obywatela a także często prywatnej

jego sfery życia i dlatego podjęcie przez Polska Izbę Ubezpieczeń, tak działań samoregulacyjnych jak i dobrych praktyk ujętych w Kodeksie, należy uznać za niezwykle ważne i zasadne.