Tom 28/2018, ss. 497-509
ISSN 1644-888X
e-ISSN 2449-7975
DOI: 10.19251/ne/2018.28(32)
www.ne.pwszplock.pl

Maria Kapturska
Państwowa Wyższa Szkoła Zawodowa w Płocku

Robert Kapturski
Państwowa Wyższa Szkoła Zawodowa w Płocku

POLITYKA UNII EUROPEJSKIEJ W KONTEKŚCIE SZEROKO POJĘTEJ WIEDZY, A BEZPIECZEŃSTWO DANYCH

EUROPEAN UNION POLICY IN THE CONTEXT OF BROADLY UNDERSTOOD KNOWLEDGE AND DATA SECURITY

Streszczenie

Autorzy skupiają się na określeniu zakresu wiedzy prawnie chronionej. Z uwagi na wprowadzane nowe przepisy, związane z ochroną danych poufnych, starają się wskazać kierunki i zagrożenia związane z codzienną działalnością w obszarze wiedzy, innowacyjności i przedsiębiorczości oraz znaleźć środki pozwalające na jasne określenie bezpiecznego przetwarzania danych. Analizują także prawne aspekty działania na danych poufnych, wykorzystując usługi usytuowane poza Polską oraz Unią Europejską. Określają podział danych na dane tajne i poufne oraz wskazują

Summary

The authors focus on defining the scope of legally protected knowledge. Due to the introduction of new regulations related to the protection of confidential data, they try to indicate the directions and risks related to daily activities in the area of knowledge, innovation and entrepreneurship and find means to clearly define secure data processing. Furthermore, they analyze legal aspects of operation on confidential data, using services located outside of Poland and the European Union. They define the division of data into secret and confidential ones,

kierunki bezpiecznego i prawnie chronionego sposobu powierzenia danych osobom trzecim i firmom z poza Unii Europejskiej. Wskazują również aspekty prawne ochrony danych, zgromadzonych w bazach wiedzy, przedsiębiorstwach oraz szeroko rozumianej wiedzy.

Słowa kluczowe: bezpieczeństwo danych, chmura obliczeniowa, administrator bezpieczeństwa Informacji.

and indicate the directions of a secure and legally protected way of entrusting data to third parties and companies from outside the European Union. They also indicate legal aspects of data protection stored in knowledge repositories, companies and broadly understood knowledge.

Keywords: data security, cloud computing, information security administrator.

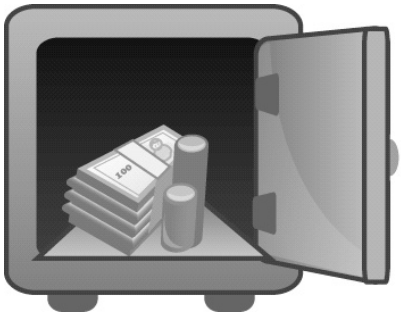
Wprowadzenie

Jak wiadomo w nowoczesnej gospodarce, opartej na wiedzy, informacja jest wymierną wartością, stanowiącą własność tak i przedsiębiorstwa, jak i osoby prywatnej. Może ona stać się cennym składnikiem wartości oraz składnikiem dodanym gotowego produktu. Biorąc pod uwagę sferę biznesową staje się ona towarem, który podlega takim samym prawom rynku, jak każdy inny produkt wytworzony w procesie biznesowym. Lecz niestety informacja nie jest objęta żadną ochroną, także z prawnego punktu widzenia. Takie podejście powoduje, że informacja traktowana przez przedsiębiorców w sposób nieadekwatny do jej wartości. Unia Europejska wprowadzając obowiązek ochrony danych, wprowadziła podział oraz zaproponowała prawną ochroną w zależności od rodzaju informacji, zgromadzonych w bazach wiedzy. Powstały w ten sposób podział wyłonił informację tajną i poufną oraz zróżnicowała ochronę ze względu na cele i mechanizmy ochrony. Mimo uświadomienia konieczności podjęcia działań związanych z poprawnym podejściem do tych dwóch typów wytworzyła pewien mechanizm odrzucenia potrzeby ochrony pozostałych stref wiedzy, zgromadzonej w przedsiębiorstwie. Należy uświadomić sobie jednak, iż pozostały obszar musi zostać objęty taką samą ochroną, jak informacje niejawne oraz należy podjąć środki ochrony adekwatne do zgromadzonej wartości intelektualnej w przedsiębiorstwie. W tym miejscu pojawia się rola Administratorów Bezpieczeństwa Informacji, którzy powinni spojrzeć na przedsiębiorstwo w sposób ogólny i zająć się obszarami do tej pory zaniedbywanymi, przez co narażającymi przedsiębiorstwo na realne straty.

1. Jakie obszary chronimy w przedsiębiorstwie

Truizmem byłoby twierdzenie, że aby rozpocząć ochronę, musimy najpierw wiedzieć, co jej podlega. Patrząc jednak na informację, takie podejście może okazać się jednak odrobinę kłopotliwe, z uwagi na to, że nie ma spójnej definicji, która mogłaby nam wskazać obszary oraz rodzaje, jakie powinny zostać objęte ochroną. Próba stworzenia jasnych ram, spowoduje zafałszowanie istoty bezpieczeństwa, przez co mogłoby to doprowadzić do paradoksu, w którym kluczowe informacje znajdujące się w majątku przedsiębiorstwa zostałyby pozbawione ochrony, natomiast te, które zostały narzucone, biorąc pod uwagę normy ogólne, pochłonęłyby duże środki finansowe, jak i czasowe, tworząc swoistą barierę, uniemożliwiającą prawidłowe funkcjonowanie przedsiębiorstwa. Można jednak spróbować wskazać kluczowe aspekty danych, które powinny zostać objęte szczególną uwagą podczas tworzenia systemów ochrony informacji.

- Informacje niejawne: W ustawie o ochronie informacji niejawnych występuje pojęcie informacji niejawnych. Określono je jako te, których ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesantów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania. Jako podstawę można tu przyjąć interes publiczny. Ochrona w tym zakresie intuicyjnie nie kojarzy się ze sferą biznesową, jednakże należy pamiętać, iż działania coraz większej ilości przedsiębiorstw, współpracujących z organami władzy publicznej i jednostkami państwowymi, zmuszają przedsiębiorcę do styczności z tego rodzajem danych. Biorąc pod uwagę środki finansowania bardzo łatwo rozszerzyć ten zakres na dane, mogące być objęte klauzulą tajności na terenie całej Unii Europejskiej [Ustawa ochronie informacji niejawnych].



Rys.1 Środki finansowe jako tajemnica przedsiębiorstwa.
Źródło: Apache OpenOffice

- Tajemnica przedsiębiorstwa: Z kolei ustawa o zwalczaniu nieuczciwej konkurencji definiuje tajemnicę przedsiębiorstwa jako nieujawnione do informacji publicznej informacje techniczne, technologiczne oraz organizacyjne przedsiębiorstwa lub inne informacje, mające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania, w celu zachowani ich poufności. Wskazuje to jednoznacznie kierunek wyznaczony interesem przedsiębiorcy, spowodowany ochroną majątku przedsiębiorcy wytworzonego podczas działania biznesowego. Jednakże widzimy wyraźnie, iż w konsekwencji uzyskanie ochrony prawnej informacji zależy, tylko i wyłącznie, od aktywnego działania przedsiębiorcy [Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej].

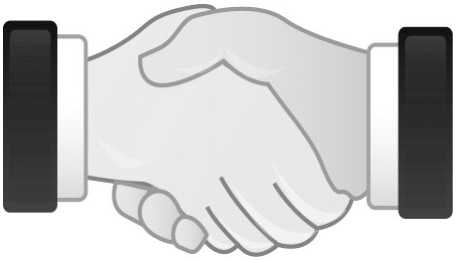
Rys.2 Dane osobowe jako dane poufne.
Źródło: Apache OpenOffice

- Dane osobowe: Kolejna istotna definicja zawarta jest w ustawie o ochronie danych osobowych, dotyczy ona danych osobowych, zawartych

w firmie. Ta część danych poufnych jest zdefiniowana jako wszelkie informacje, dotyczące osoby fizycznej, pozwalające w jednoznaczny sposób zidentyfikować osobę. Ochrona tych danych jest jak najbardziej uzasadniona, gdyż pozwala w sposób oczywisty chronić autonomię oraz prywatność osoby, pozwolić jej w jednoznaczny sposób decydować o tym, w jakim stopniu jej wizerunek zostanie upubliczniony. W praktyce każda firma w sposób świadomy lub nie przetwarza dane osobowe [Ustawa o ochronie danych osobowych].

Rys.3 Tajemnice branżowe rozumiane w kategorii prawa
Źródło: Apache OpenOffice

- Tajemnice branżowe i zawodowe: Poza powyższymi kategoriami prawo określa szereg innych tajemnic zdefiniowanych w ustawach, regulujących poszczególne rodzaje działalności gospodarczej lub zawodowej. Tajemnice zawodowe są ściśle związane z wykonywanym zawodem, zazwyczaj są to zawody wymagające szczególnych kwalifikacji i związanych z dostępem do specyficznej informacji. Możemy w tym zakresie wyróżnić takie zawody, jak: lekarz, radca prawny, itp. gdzie wykonujący zawód, ma dostęp do danych, które są mu niezbędne do rozwiązania problemu, co z kolei, w sposób oczywisty łączy się w prostej linii z jego wykonywanym zawodem. Natomiast tajemnice branżowe są związane z określonej kwalifikacji działalności, którą w odróżnieniu od działalności zawodowej wykonuje podmiot, niebędący osobą fizyczną. Do zachowania tajemnicy jest zobowiązany podmiot, wykonujący działalność. Nie należy zapominać, iż w skład podmiotu wchodzą pracownicy, którzy z uwagi na wykonywanie działań na informacji niejawnej także powinni być zobowiązani do utrzymania polityki firmy, w stosunku do podejścia do danej informacji. Przykładem mogą tu być instytucje bankowe lub prawnicy zrzeszeni w kancelarii prawnej.



Rys.4 Powierzanie tajemnic.
Źródło: Apache OpenOffice

Nie należy jednak zapominać o innych tajemnicach chronionych prawnie, występujących w działalności, tak na przykład tajemnica negocjacji określona w kodeksie cywilnym.

2. Modele ochrony prawnej

Rys.5 Modele ochrony prawnej
Źródło: Apache OpenOffice

Przepisy prawa określają kilka poziomów ochrony prawnej informacji niejawnych. Pierwszym z nich jest ochrona publicznoprawna, która jest realizowana za pomocą narzędzi prawa publicznego, ta z kolei jest realizowana na podstawie prawa publicznego. Jej zadaniem jest w pierwszym rzędzie zaspokojenie interesu publicznego, ale jednocześnie chroni interesy osób fizycznych w stosunkach z organami władzy. Prawo to wynika, w sposób bezpośredni, z konstytucji i stanowi zapewnienie autonomii jednostki wobec państwa. Wynika z niej wprost, np. ochrona danych osobowych, która jest realizowana

głównie przy użyciu narzędzi prawa administracyjnego. W ramach prawa publicznego najmocniejsza jest ochrona karna, przewidująca nawet kary pozbawienia wolności.

Rys. 6 Poziom ochrony prawnej
Źródło: Apache OpenOffice

Drugim poziomem ochrony prawnej jest ochrona prywatnoprawna. Jest ona oparta na przesłaniu, mającym na celu ochronę interesu prywatnego. Jest ona realizowana na zasadzie równorzędności podmiotów. Podstawa ta pozwala na ochronę podmiotów, na podstawie ustawy o zwalczaniu nieuczciwej konkurencji. Pozwala ona na dochodzenie praw w procesie cywilno-prawnym od naruszenia tajemnicy. Możemy, na jej podstawie, domagać się zaniechania niedozwolonych działań, usunięcia ich skutków, wydania bezpodstawnie uzyskanych korzyści lub zapłaty odszkodowania. Na poziomie prywatnym chronione są też naruszenia tajemnicy udostępnionej kontraktowo. W umowie o udostępnieniu danych musi znaleźć się klauzula poufności, przez co podmiot udostępniający może domagać się odszkodowania, przewidzianego w klauzuli, obejmującej kary umowne na wypadek udostępnienia lub nieprawnego wykorzystania danych.

3. Praktyczne aspekty ochrony danych.

Powyższe definicje pokazują w przejrzysty sposób aspekty ochrony danych. Należy jednak pamiętać, aby w oczywisty sposób zdefiniować aspekty ochrony naszych danych. Pamiętając o tym, iż stosowanie jakichkolwiek szablonów może być zgubne już w samych założeniach. Musimy pamiętać o zdefiniowaniu poziomów ochrony, a także o podziale poprzez ich kategoryzację na ściśle tajne, tajne, poufne i zastrzeżone. Kolejnym wydawałoby się oczywistym krokiem, jest wprowadzenie środków ochrony, począwszy od fizycznej, bezpieczeństwa informatycznego oraz odpowiednich procedur postępowania z informacjami. Pamiętajmy jednak, że prowadząc działalność gospodarczą

możemy wejść w posiadanie danych mogących mieć wpływ na bezpieczeństwo Państwa, a nawet Unii Europejskiej. Biorąc pod uwagę, iż zawsze możemy zostać postawieni przed faktem niedostatecznej aktywności, w ochronie danych osobowych, musimy zwrócić szczególną uwagę na politykę kreowania naszego wizerunku, w sposób przejrzysty i udostępniać bez ograniczeń dane, które mają na celu prawidłowe funkcjonowanie naszego przedsiębiorstwa, jednocześnie monitorując, jak daleko idące wnioski można wyciągnąć z informacji, przedstawionych publicznie. Niestety należy także zastosować środki ostrożności, opierające się na podstawach funkcjonowania, czy to przedsiębiorstwa czy to osoby fizycznej. Najbardziej zagrożonym aspektem naszego postępowania może okazać się system informatyczny, gdyż, przy dzisiejszym rozwoju techniki, jest on główną składnicą naszych informacji.

4. Zagrożenia związane z systemem informatycznym.

Oczywiste wydaje się stwierdzenie, iż najsłabszy punk systemu bezpieczeństwa jest miarą całego systemu. Tak więc, bez żadnego powątpiewania, można powiedzieć, że wprowadzanie danych tajnych do szerokiego grona przedsiębiorczości, jakie następuje w ostatnich latach na terenie Rzeczypospolitej Polskiej jest swoistą elipsą uderzającą w podstawy bezpieczeństwa Unii Europejskiej. Poprzez usługi dostarczane nam coraz szerzej jako wydawałoby się dodatkowe „bonusy" firm informatycznych, pomagające nam w życiu codziennym, narażamy się na ataki pozostając bez żadnej obrony, a nasze działania, podjęte w celu zabezpieczenia istotnych dla nas aspektów, pozostają otwarte dla osób, którym informacje te mogą stać się przydatne. Przykładem takiego działania może być przetwarzanie danych w chmurze. Jeżeli możemy mieć zaufanie do firm, które działają w dobrej wierze, tak należy się zastanowić nad intencjami przedsiębiorstw, próbujących wdrożyć usługę w naszym przedsiębiorstwie bez naszej zgody.

5. Czym jest chmura?

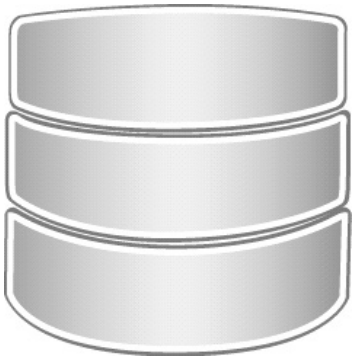
Rys. 7 Powierzenie danych osobom trzecim
Źródło: Apache OpenOffice

Sama nazwa wzięła się stąd, że w infografikach biznesowych, internet przedstawiany był w postaci chmury (ang. cloud). Jednak niestety, chociaż większość społeczeństwa słyszała o chmurze, jak pokazuje badanie przeprowadzone przez Wakefield Reserch w 2012 roku wynika, że aż 22% społeczeństwa tylko udaje, że wie, czym tak naprawdę jest *cloud computing,* chociaż 33% badanych mówi o tym w pracy, 14% na rozmowach kwalifikacyjnych, a co ciekawe, 17% podczas pierwszej randki. Możliwe, że problem zdefiniowania pojęcia chmury obliczeniowej wynika z tego, iż obejmuje stale ewoluującą liczbę usług z sektora IT [www2].

Idea chmury opracowana na początku XX wieku przez Henrego Forda pokazywała rozwój tego sektora, jako kierunek usprawnionego podejścia do zarządzania zasobami przedsiębiorstwa, twierdził on iż *„Jeśli jest coś, czego nie potrafimy zrobić wydajniej, taniej i lepiej niż inni, nie ma sensu, żebyśmy to robili i powinniśmy zatrudnić do tej pracy kogoś, kto zrobi to lepiej niż my”* dzisiaj moglibyśmy to nazwać outsoursingem.

Cloud Computing jest dokładnym urzeczywistnieniem tej idei, ponieważ zamiast budować całą infrastrukturę informatyczną, możemy powierzyć nasze dane firmom, które przetworzą je w swojej infrastrukturze, co z kolei umożliwi nam nietworzenie infrastruktury IT w naszym przedsiębiorstwie.

6. Przetwarzanie danych poufnych w chmurze



Rys.8 Przetwarzanie danych w chmurze
Źródło: Apache OpenOffice

Biorąc pod uwagę coraz szersze zainteresowanie przedsiębiorstw przetwarzaniem danych poza siedzibą firmy zarówno do celów biznesowych, jak i w celach działalności statutowych firmy możemy założyć, że prawie na pewno znajdą się w niej dane poufne, a nawet tajne. Analizując działanie przedsiębiorstw, widzimy, że chmura otacza nas z każdej strony, czy gdy robimy przelew bankowy lub po prostu korzystamy z aplikacji mobilnych w celu uproszczenia sobie codziennego funkcjonowania w przedsiębiorstwie. Nie zastanawiamy się czy dane wysyłane do jakże często nie znanego nam przedsiębiorcy, mogą zawierać się w którejkolwiek z dziedzin, zawartych w punkcie drugim tej publikacji. I tu pojawia się zasadnicze pytanie „*Co na to prawo?”*. Czy dane sensytywne mogą być przetwarzane w modelu chmury obliczeniowej, na niezidentyfikowanych serwerach dostawcy usługi?

Spoglądając na szeroki zakres danych, jakie mogą zagrozić bezpieczeństwu naszego przedsięwzięcia biznesowego, postaram skupić się na jednym przykładzie, w celu naświetlenia problemu, który będzie dotyczył coraz większej ilości instytucji z sektora prywatnego, jak i publicznego.

Skupię się na aspekcie danych poufnych, który dotyczy każdego członka społeczności międzynarodowej, niezależnie od pochodzenia, wyznania czy poglądów politycznych. Są to dane osobowe. Definicja danych osobowych, która znajduje się w art. 6 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych mówi: *„Dane osobowe to wszystkie informacje, które umożliwiają identyfikację osoby fizycznej bez nadmiernych kosztów, czasu i działań”. [Ustawa o ochronie danych osobowych1]*

Rys. 9 Ochrona danych osobowych jako danych poufnych
Źródło: Apache OpenOffice

Należy przeanalizować, w ramach jakiej części prawnych aspektów się poruszamy, a więc podstawą do analizy są przede wszystkim: *„Unijna dyrektywa 95/45/WE Parlamentu Europejskiego i Rady WE”* oraz jej pochodna – Polska ustawa *„O ochronie danych osobowych”.* Musimy jednak pamiętać iż unijna dyrektywa została przygotowana w połowie lat 90. Z perspektywy technologii informatycznych to bardzo długi czas. Możemy więc jednoznacznie powiedzieć, iż ogromna część przepisów w niej zawartych straciła na aktualności. Jednak funkcjonowanie jednolitej dyrektywy, na całym terytorium Unii Europejskiej, ma też ogromną zaletę. Pozwala bowiem na ujednolicenie obowiązujących przepisów. Każda krajowa ustawa w zakresie danych osobowych musi chronić je co najmniej na takim samym poziomie, jak unijna dyrektywa. Niestety polska ustawa o ochronie danych osobowych jest jej niemal wierną kopią, jakby nie zauważając zmian w otoczeniu biznesowym.

Analizując dalej dyrektywę unijną pod względem przetwarzania danych w chmurze, możemy odnaleźć zapis mówiący o *„operacji powierzenia przetwarzania danych osobowych”* art.31 ustawy, art 17 Dyrektywy 95/46/WE [Ustawa o ochronie danych osobowych, Dyrektywy europejskie].

Analizując powyższy schemat można powiedzieć, iż firma A, która jest Administratorem danych osobowych i decyduje o celach i środkach ich przetwarzania, powierza dane osobowe firmie B, którą możemy nazwać procesorem (ang. processor), ta z kolei, na podstawie zlecenia, może przetwarzać dane osobowe jedynie w celu realizacji powierzonego zadania i w taki sposób w jaki zostało to uprzednio ustalone. Spoglądając na ustawę możemy powiedzieć, iż firma A powierza dane osobowe firmie B. Należy jednak pamiętać, że takie powierzenie powinno być udokumentowane zawarciem, tzw. umowy

powierzenia danych osobowych (art. 31 ustawy oraz art.17 pkt 3 Dyrektywy 95/46/WE). Główny Inspektor Ochrony Danych Osobowych stoi na stanowisku, że taka umowa powinna zostać zawarta w formie pisemnej mimo, że występują w tej części pewne spory doktryny prawnej. W praktyce zwarcie umowy powierzenia z firmą prowadzącą działalność, związaną z przetwarzaniem w chmurze, jest bardzo trudne, ponieważ przedsiębiorcy nie chcą przejmować odpowiedzialności za wyciek danych, a ustawodawca nie nałożył na nich obowiązku przejęcia odpowiedzialności. To na Administratorze Danych będzie spoczywać cała odpowiedzialność, jednakże może on dochodzić swoich praw przed Generalnym Inspektorem Ochrony Danych Osobowych.

7. Przetwarzanie w chmurze na terenie Europejskiego Obszaru Gospodarczego

Rys. 10 Przetwarzanie danych w chmurze na terenie Europejskiego Obszaru Gospodarczego i poza nim.

Źródło: Apache OpenOffice

Jednolite przepisy, obowiązujące na terenie całego Europejskiego Obszaru Gospodarczego, pozwalają na powierzanie danych bez obawy o nieprzestrzeganie dyrektywy. A więc poza państwami Unii Europejskiej także w Norwegii, Islandii i Liechtensteinie. Sytuacja staje się bardziej skomplikowana, gdy chcemy powierzyć dane tak zwanym państwom trzecim reguluje to art.47 Dyrektywy 95/46/WE. Znacząco ułatwione zostało powierzanie danych Stanom Zjednoczonym, które są ojczyzną Cloud Computing, tworząc porozumienie Safe Harbour, zatwierdzonego prze Unię Europejską decyzją Komisji 2000/520/WE z dnia 26 lipca 2000 roku (O.J. L 215,25.08.2000 s. 0007-0047).

W skrócie wszystkie firmy ze Stanów Zjednoczonych, które zostały umieszczone na liście [www1], traktowane są jak podmioty z Europejskiego Obszaru Gospodarczego. Na liście oczywiście znajdują się tacy giganci, jak Google czy Microsoft. Niestety, powierzenie danych firmom ze Stanów

Zjednoczonych łączy się z ryzykiem, związanym z niejasnościami związanymi z powiązaniami gigantów informatycznych z National Security Agency (NSA) i ogromną skalą monitorowania internetu przez Agencję.

8. Zagrożenia a stan prawny

W obecnym stanie prawnym przetwarzanie oraz udostępnianie danych poufnych jest legalne. Należy jednak pamiętać o dwóch ważnych elementach:

- umowie powierzenia,
- powierzeniu danych firmie, działającej na terenie Europejskiego Obszaru Gospodarczego lub posiadającej ważny certyfikat Safe Harbour.

Jednakże nie należy zapominać, iż każde powierzenie danych może wpłynąć negatywnie na stan bezpieczeństwa naszej organizacji oraz o tym, że dane mogą być wykorzystywane bez naszej wiedzy, co z kolei może negatywnie wpłynąć na wynik finansowy przedsięwzięcia.

Literatura

Ustawa z dnia 29 sierpnia 1997 r. O ochronie danych osobowych. Dz.U. 1997 nr 133 poz. 883.

Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 26 czerwca 2003 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zwalczaniu nieuczciwej konkurencji Dz.U. 2003 nr 153 poz. 1503.

Dyrektywy europejskie Dz.U. 2005 nr 178 poz. 1480.

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Dz.U. 2010 nr 182 poz. 1228.

[www1] http://safeharbor.com/list.asp (dostęp: 26.02.2018)

[www2] http://www.wakefieldresearch.com (dostęp 26.02.2018)