

SŁOWNICZEK POJĘĆ

Internet – jest jednym z najpotężniejszych i najszybciej rozwijających się mediów na świecie. Ten system komunikacyjny, mający w swej istocie stanowić początkowo środek łączności, stanowi obecnie jedno z podstawowych źródeł informacji dla większości społeczeństwa. Jego poprzednikiem była pierwsza sieć rozległa ARPANET, która powstała z inicjatywy Pentagonu. W 1980 r. została rozdzielona na ARPANet i Milnet. Całość otrzymała nazwę DARPAInternet, która z czasem została skrócona do powszechnie obecnie używanego terminu Internet. Przełomowy dla dalszego rozwoju był rok 1989, kiedy brytyjski programista Tim Berners – Lee wymyślił sposób, aby wszelkie informacje krążące w sieci ujęte zostały w formie jednorodnych dokumentów. Jego projekt nazwany został World Wide Web (WWW) od 1992 r. stał się on nierozłącznym elementem cyberprzestrzeni. W efekcie obecnie zawartość strony internetowej obejmuje nie tylko tekst pisany, ale także m. in. zdjęcia, filmy i dźwięki.

Off-line (ang. *odłączony od linii*) – określa sposób oglądania materiałów pobranych z Internetu bądź innej sieci komputerowej. Tryb off-line jest formą działania użytkownika sieci po odłączeniu elementów współpracujących z siecią, określa np. stan w wyniku przerwania połączenia z Internetem po załadowaniu określonej strony WWW (przeglądarka WWW pozostaje wówczas w stanie off-line). Określenia „off-line” można używać także do opisu sytuacji przygotowywania pewnych materiałów bez utrzymywania połączenia z siecią Internet, a które później mają zostać przesłane za pośrednictwem Internetu (czyli on-line). W przypadku łączy służących do przesyłania informacji zestawianych dopiero wówczas, gdy zachodzi potrzeba ich użycia, tryb off-line umożliwia zmniejszenie kosztów ponoszonych przez użytkownika tych sieci. W telefonach komórkowych mianem off-line oznacza się opcję odłączenia wszelkich usług umożliwiających połączenie z innym urządzeniem. Terminem o przeciwnym znaczeniu jest online¹.

On-line (z ang. dosł. *na linii*) – zwykle status osoby, serwera lub innego przedmiotu związanego z dostępem do Internetu, który informuje o dostępności – aktywności. Przeciwnością trybu on-line jest tryb off-line².

Środki komunikacji elektronicznej – pojęcie to zostało zdefiniowane w sposób funkcjonalny w Ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. Nr 144, poz. 1204 ze zm.). Pod tym pojęciem należy rozumieć rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy

wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztą elektroniczną. Przyjmuje się, że określenie „indywidualne” oznacza wymianę danych pomiędzy ich odbiorcami, które nie przewiduje dalszego pośredniczenia w porozumiewaniu się. W szczególności wyżej wskazane kryteria spełnia poczta elektroniczna (komunikacja pomiędzy indywidualnie określonymi użytkownikami), strona WWW (komunikacja pomiędzy nadawcą a nieokreśloną grupą odbiorców), forum dyskusyjne (komunikacja pomiędzy wieloma użytkownikami), interaktywny formularz (komunikacja pomiędzy wieloma nadawcami a jednym odbiorcą). Środki komunikacji elektronicznej służą do przesyłania informacji na odległość. Przykładowe środki komunikacji elektronicznej: poczta elektroniczna, komunikatory internetowe, telefonia internetowa.

Informatyczny nośnik danych – materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej (art. 3 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. Nr 64, poz. 565 z późn. zm.) Informatyczny nośnik danych jest przedmiotem fizycznym, na którym możliwe jest zapisanie informacji, i z którego możliwe jest późniejsze odczytanie tej informacji. Pojęcie nośnika danych jest ściśle związane z informatyką i komputerami. Każdy nośnik danych charakteryzuje określona gęstość zapisu, wynikająca z jego właściwości fizycznych³. Przykładowe nośniki danych: dysk, pendrive, płyta CD, płyta DVD.

System teleinformatyczny – zgodnie z art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. Nr 64, poz. 565 z późn. zm.) zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający: przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.). Jest to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. Na systemy informatyczne składają się obecnie takie elementy jak: 1) sprzęt – obecnie głównie komputery oraz urządzenia służące do przechowywania danych, urządzenia służące do komunikacji między sprzętowymi elementami systemu, urządzenia służące do komunikacji między ludźmi a komputerami, urządzenia służące do odbierania danych ze świata zewnętrznego – nie od ludzi (np. czujniki elektroniczne, kamery, skanery), urządzenia służące do wywierania wpływu przez systemy informatyczne na świat ze-

1 Zob. <http://pl.wikipedia.org/wiki/Offline>, a także P. Adamczewski, *Słownik informatyczny*, Gliwice 2005, s. 146.

2 Zob. <http://pl.wikipedia.org/wiki/Online>.

3 Zob. http://pl.wikipedia.org/wiki/No%C5%9Bnik_danych.

wewnętrzny – elementy wykonawcze (na przykład silniki sterowane komputerowo, roboty przemysłowe, podłączony do komputera ekspres do kawy, sterowniki urządzeń mechanicznych), urządzenia służące do przetwarzania danych niebędące komputerami, 2) oprogramowanie, 3) zasoby osobowe – ludzie, 4) elementy organizacyjne – czyli procedury (procedury organizacyjne – termin z zarządzania) korzystania z systemu informatycznego, instrukcje robocze itp., 5) elementy informacyjne; bazy wiedzy – ontologie dziedzin, w których używany jest system informatyczny – np. podręcznik księgowania w wypadku systemu finansowo-księgowego⁴.

Dokument elektroniczny – w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz.565 ze zm.) stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych. Dokument elektroniczny jest efektem działania aplikacji użytkowej (programu użytkowego przeznaczonego do realizacji określonych zadań, np. edytor tekstu, arkusz kalkulacyjny) i jest wyświetlany na ekranie monitora i/lub zapisany na dysku (informatycznym nośniku danych). Tym samym jest to dokument zapisany jako plik (tekstowy, muzyczny, graficzny, etc.), który został utwalony w sposób umożliwiający jego zapisanie, a następnie odczytanie jego zawartości.

Zapis – zgodnie z treścią rozporządzenia Ministra Sprawiedliwości z dnia 10 sierpnia 2011 r. w sprawie zapisu dźwięku albo obrazu i dźwięku z przebiegu posiedzenia jawnego (Dz. U. Nr 175, poz.1046) pod tym pojęciem należy rozumieć realizowane w systemie teleinformatycznym utrwalenie obrazu i dźwięku (lub wyłącznie dźwięku) z wszystkich czynnych urządzeń utrwalających obraz i dźwięk. Inaczej rzecz ujmując pod tym pojęciem należy rozumieć finalny efekt przeprowadzonego procesu utrwalenia przebiegu posiedzenia jawnego, którym jest nagranie obrazu i dźwięku (lub wyłącznie dźwięku) zapisane w postaci jednego pliku, umożliwiającego wielokrotne odtwarzanie jego treści przy wykorzystaniu różnych nośników, w tym za pośrednictwem systemu teleinformatycznego.

Plik – zbiór danych w sposób jednoznaczny odróżniający się od innych danych, opisany przy wykorzystaniu zindywidualizowanej nazwy.

Adnotacje – szczegółowo zagadnienie to zostało omówione w rozporządzeniu Ministra Sprawiedliwości z dnia 10 sierpnia 2011 r. w sprawie zapisu dźwięku albo obrazu i dźwięku z przebiegu posiedzenia jawnego (Dz. U. Nr 175, poz.1046). Pod tym terminem należy rozumieć dokument elektroniczny, powiązany z zapisem i zawierający informacje dotyczące przebiegu posiedzenia jawnego. Adnotacje dzielą się na dwie grupy, tzn. adnotacje publiczne, które obejmują również elementy tzw. protokołu skróconego, oraz adnotacje prywatne. Ich rola w późniejszej pracy nad nagraniem jest nieoceniona. Przyjmuje się nazywać je swoistym „spisem treści” nagrania, które później zapewnia efektywną pracę z zapisem.

Certyfikat – zgodnie z ustawą z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz.1450 ze zm.) jest to elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.

Certyfikat kwalifikowany – zgodnie z ustawą z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz.1450 ze zm.) jest to certyfikat spełniający warunki określone w ustawie, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający wymogi określone w ustawie. Gwarantuje wysoki poziom bezpieczeństwa. Bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu jest równoważny pod względem skutków prawnych podpisowi własnoręcznemu, o ile przepisy szczególne nie stanowią inaczej (art.5 ust.2 ustawy o podpisie elektronicznym).

Transkrypcja – pod tym terminem należy rozumieć zapisanie w sposób dosłowny tekstu mówionego przy zachowaniu ścisłego odwzorowania głosek za pomocą liter i znaków graficznych (inaczej: pisownia fonetyczna).

Metadane – zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz. U. Nr 206, poz.1517) – zestaw logicznie powiązanych z dokumentem elektronicznym usystematyzowanych informacji opisujących ten dokument, ułatwiających jego wyszukiwanie, kontrolę, zrozumienie i długotrwałe przechowanie oraz zarządzanie. Niezbędnymi elementami struktury dokumentów elektronicznych są następujące metadane:

- 1) identyfikator – jednoznaczny w danym zbiorze dokumentów znacznik dokumentu, który umożliwia jego identyfikację;
- 2) twórca – podmiot odpowiedzialny za treść dokumentu, z podaniem jego roli w procesie tworzenia lub akceptacji dokumentu;
- 3) tytuł – nazwa nadana dokumentowi;
- 4) data – data zdarzenia związanego z tworzeniem dokumentu;
- 5) format – nazwa formatu danych zastosowanego przy tworzeniu dokumentu;
- 6) dostęp – określenie komu, na jakich zasadach i w jakim zakresie można udostępnić dokument;
- 7) typ – określenie podstawowego typu dokumentu (np. tekst, dźwięk, obraz, obraz ruchomy, kolekcja) w oparciu o listę typów Dublin Core Metadata Initiative i jego ewentualne dookreślenie (np. prezentacja, faktura, ustawa, notatka, rozporządzenie, pismo);
- 8) relacja – określenie bezpośredniego powiązania z innym dokumentem i rodzaju tego powiązania;
- 9) odbiorca – podmiot, do którego dokument jest adresowany;
- 10) grupowanie – wskazanie przynależności do zbioru dokumentów;
- 11) kwalifikacja – kategoria archiwalna dokumentu;
- 12) język – kod języka naturalnego zgodnie z normą ISO-639-2 lub inne określenie języka, o ile nie występuje w normie;

⁴ Zob. http://pl.wikipedia.org/wiki/System_informatyczny.

- 13) opis – streszczenie, spis treści lub krótki opis treści dokumentu;
- 14) uprawnienia – wskazanie podmiotu uprawnionego do dysponowania dokumentem.

Dla każdego dokumentu elektronicznego podaje się wartości metadanych określonych w pkt 1-7. Wartości metadanych, o których mowa w pkt 8-14, podaje się, jeżeli zostały przypisane do dokumentu w procesie jego tworzenia, przetwarzania lub przechowywania. Dokumenty elektroniczne należy zapisać w strukturze umożliwiającej automatyczne wyodrębnienie treści dokumentu oraz poszczególnych metadanych. Umieszczanie w strukturze dokumentu elektronicznego innych metadanych nie może wpływać na zmianę wartości niezbędnych metadanych ani utrudniać ich automatycznego wyodrębniania⁵. Metadane można określić ogólnie jako dane o danych, którymi są np. klasyczne katalogi biblioteczne. Przy pomocy metadanych opisywane są dokumenty elektroniczne, w szczególności dokumenty dostępne poprzez sieci komputerowe, np. strony WWW dostępne w sieci Internet, jak również dokumenty tworzące nowoczesne biblioteki cyfrowe.

Podpis elektroniczny – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny (art.3 pkt 1 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, Dz. U. Nr 130, poz.1450 z późn. zm.) Podpis elektroniczny można określić jako matematyczny sposób potwierdzania autentyczności cyfrowego dokumentu. Konstrukcja podpisu elektronicznego bazuje na algorytmach szyfrowania z kluczem publicznym. Podstawą działania tego typu szyfrów są dwa klucze występujące w parze: klucz prywatny oraz powiązany z nim klucz publiczny. Klucz prywatny, przyporządkowany tylko właścicielowi podpisu elektronicznego, dla zachowania bezpieczeństwa musi pozostać pod wyłączną kontrolą jego właściciela, zaś klucz publiczny wraz z informacjami o właścicielu w postaci certyfikatu klucza publicznego jest udostępniany wszystkim zainteresowanym. W dużym uproszczeniu do składania podpisów elektronicznych wykorzystuje się klucz prywatny, zaś do weryfikacji podpisu (sprawdzenia, kto podpisał dokument podpisem elektronicznym) można użyć tylko i wyłącznie klucza publicznego pochodzącego z danej pary. Dzięki tej własności podpis elektroniczny pozwala jednoznacznie ustalić, kto jest autorem podpisanego dokumentu⁶.

Podpis elektroniczny służy zapewnieniu między innymi następujących funkcji: 1) autentyczności, czyli pewności co do autorstwa dokumentu, 2) niezaprzeczalności nadania informacji, co oznacza, że nadawca wiadomości nie może wyprzec się wysłania wiadomości, gdyż podpis cyfrowy stanowi dowód jej wysłania (przy czym istnieją także inne rodzaje niezaprzeczalności), 3) integralności, czyli pewności, że wiadomość nie została zmodyfikowana po złożeniu podpisu przez autora. Do zapewnienia wszystkich wymienionych funkcji potrzebne jest zastosowanie trzech środków: 1) instrumentów technicznych – algorytmów, protokołów i formatów, które dzięki zastosowaniu technik krypto-

graficznych zapewniają integralność oraz wiążą klucz prywatny autora z dokumentem, zapewniając autentyczność i niezaprzeczalność, 2) instrumentów prawnych, czyli dyrektyw, ustaw i rozporządzeń, które osadzają wymienione instrumenty techniczne w obowiązującym prawie, 3) instrumentów organizacyjnych, takich jak centra certyfikacji, które występując jako zaufana trzecia strona poświadczają związek klucza prywatnego z konkretną osobą⁷.

Bezpieczny podpis elektroniczny – zgodnie z art.3 pkt 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz.1450 z późn. zm.) jest to podpis elektroniczny, który: a) jest przyporządkowany wyłącznie do osoby składającej ten podpis, b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego, c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakkolwiek późniejsza zmiana tych danych jest rozpoznawalna. W praktyce złożenie bezpiecznego podpisu elektronicznego jest stosunkowo proste. Aby to zrobić trzeba się zaopatrzyć w zestaw do jego składania. Na podstawowy zestaw składa się: certyfikat kwalifikowany, karta kryptograficzna, aplikacja do składania i weryfikacji bezpiecznych podpisów elektronicznych oraz czytnik kart. Sam proces złożenia podpisu polega na wskazaniu dokumentu do podpisania i postępowaniu zgodnie z zaleceniami aplikacji, która poprosi o włożenie karty do czytnika i podanie kodu PIN, co pozwoli, przy pomocy klucza prywatnego zapisanego na karcie wygenerować podpis elektroniczny pod wskazanym dokumentem⁸. Zalety korzystania z podpisu elektronicznego: 1) unikalność – każdy dokument elektroniczny posiada unikalny podpis elektroniczny ściśle związany z danym dokumentem. Nie można zatem podpisu elektronicznego przygotowanego dla danego dokumentu dołączyć do innego dokumentu. Taka manipulacja zostanie wykryta w momencie weryfikacji podpisu elektronicznego, 2) integralność – jakkolwiek zmiana dokumentu opatrzonego podpisem elektronicznym zostanie automatycznie wykryta w momencie weryfikacji przez odbiorcę podpisu elektronicznego dołączonego do dokumentu. Co ważne, w przeciwieństwie do podpisu własnoręcznego weryfikacja podpisu elektronicznego zostanie wykonana w aplikacji i nie wymaga żadnej specjalistycznej wiedzy od osoby, która weryfikuje podpis, 3) niezaprzeczalność – tylko osoba posiadająca dane służące do składania podpisów, czyli tzw. klucz prywatny, korespondujący z danymi zawartymi w certyfikacie, mogła wygenerować podpis elektroniczny pod danym dokumentem, 4) potwierdzenie tożsamości – dane osoby składającej podpis elektroniczny zawarte w certyfikacie zostały potwierdzone przez podmiot świadczący usługi certyfikacyjne. Jeżeli podpis elektroniczny został pozytywnie zweryfikowany, mógł on zostać złożony jedynie przez osobę wskazaną w certyfikacie, która posiadała klucz prywatny tworzący z danym kluczem publicznym jedną parę. Dzięki tym zaletom podpis elektroniczny zapewnia bezpieczną i niezaprzeczalną komunikację w sieci internetowej⁹.

⁷ Zob. http://pl.wikipedia.org/wiki/Podpis_cyfrowy.

⁸ Zob. http://www.kir.com.pl/main.php?p=podpis_elektroniczny&gclid=CP3Kxcer-aoCFYL-wzAodjyK5Eg.

⁹ Zob. http://www.kir.com.pl/main.php?p=podpis_elektroniczny&gclid=CP3Kxcer-aoCFYL-wzAodjyK5Eg.

⁵ Zob. także rozporządzenie Ministra Sprawiedliwości z dnia 10 sierpnia 2011 r. w sprawie zapisu dźwięku albo obrazu i dźwięku z przebiegu posiedzenia jawnego (Dz. U. Nr 175, poz. 1046).

⁶ Zob. http://www.kir.com.pl/main.php?p=podpis_elektroniczny&gclid=CP3Kxcer-aoCFYL-wzAodjyK5Eg.

Bezpieczne urządzenie służące do składania podpisu elektronicznego – zgodnie z art.3 pkt 7 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz.1450 z późn. zm.) urządzenie służące do składania podpisu elektronicznego spełniające wymagania określone w ustawie. Zob. także rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 roku w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz. U. Nr 128 poz.1094). Składa się z oprogramowania podpisującego oraz współpracującego z nim komponentu technicznego (np. karta kryptograficzna). Bezpieczne urządzenie powinno posiadać certyfikat bezpieczeństwa odpowiedniego poziomu, znajdować się na liście bezpiecznych urządzeń oraz posiadać odpowiednie deklaracje zgodności. Informacje na temat konkretnych zestawów bezpiecznych urządzeń można znaleźć na stronach internetowych kwalifikowanych podmiotów świadczących usługi certyfikacyjne (rejestr tych podmiotów dostępny jest na stronie internetowej Narodowego Centrum Certyfikacji: http://www.nccert.pl/ncc/rejestr/rejestr_index.aspx).

CENTRUM BADAŃ PROBLEMÓW PRAWNYCH I EKONOMICZNYCH KOMUNIKACJI ELEKTRONICZNEJ (CBKE)

Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej (CBKE) jest jednostką naukowo-badawczą działającą w ramach Uniwersytetu Wrocławskiego. Jednostka ta powołana została w celu prowadzenia badań naukowych nad: umowami elektronicznymi, prawem telekomunikacyjnym, przestępczością komputerową, ochroną danych osobowych przetwarzanych informatycznie, stosowaniem technik informatycznych w wymiarze sprawiedliwości, ochroną własności intelektualnej w Internecie, ideą elektronicznego rządu, informatyką prawniczą, prawem mediów oraz prawnymi aspektami dostępu do informacji.

Początek XXI wieku to okres bujnego rozwoju tzw. technologii IT, co spowodowało, że założenie CBKE pokryło się z dynamicznie wzrastającym zainteresowaniem tą tematyką. Kolejne lata funkcjonowania na Wydziale ugruntowały naszą pozycję jako solidnego organizatora i współorganizatora przedsięwzięć naukowo-badawczych.

Priorytety naszego działania obejmują m. in. prowadzenie w ramach i pod kierownictwem Uczelni prac naukowo-badawczych, rozwijanie międzynarodowych kontaktów i współpracy naukowej, nawiązywanie współpracy z innymi organizacjami i ośrodkami akademickimi zajmującymi się pokrewną tematyką, jak również rozwijanie i kształtowanie życia naukowego wśród studentów oraz integracja środowiska studenckiego i naukowego.

Kierownikiem CBKE jest prof. dr hab. Jacek Gołaczyński. Zespół Centrum stanowią pracownicy naukowcy Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego oraz doktoranci prawa. Doktoranci prowadzą badania naukowe pod kierunkiem Rady Naukowej CBKE składającej się z siedmiu profesorów naszego Wydziału oraz profesora z Uniwersytetu w Hanowerze. Przewodniczącym Rady jest Dziekan Wydziału dr hab. prof. Włodzimierz Gromski.

VNT LAW & COMMUNICATIONS SPÓŁKA Z O.O.

VNT Law & Communications spółka z o.o. organizuje seminaria otwarte (terminarz szczegółowy vnt.com.pl) ale także dedykowane wysoko specjalistyczne seminaria zamknięte dla sądów (zarówno okręgowych jak rejonowych), okręgowych rad radców prawnych, adwokackich, kancelarii prawnych, urzędów, przedsiębiorców itp. Wykładowcami są uznani specjaliści zarówno naukowcy, jak sędziowie, wysokiej rangi urzędnicy, a także praktycy. Oprócz seminariów z prawa, jako jeden z nielicznych podmiotów w kraju, organizujemy dla małych grup (np. w ramach danej izby korporacyjnej, sądu okręgowego itp.) specjalistyczne zajęcia z prawniczego języka angielskiego (współpraca z Londyńską Izbą Przemysłowo Handlową w zakresie certyfikowania znajomości specjalistycznego języka angielskiego). Realizujemy aktualnie projekty współfinansowane ze środków UE.

Aktualnie realizowane szkolenia dedykowane (możliwość realizacji dla poszczególnych korporacji czy też sądów):

- Elektroniczne postępowanie upominawcze
- Wpływ najnowszych zmian w k.p.c. na postępowanie sądowe
- Konsekwencje zmian k.p.c. dla funkcjonowania sądu i pełnomocników w związku z e-protokołem
- Nowa regulacja hipoteki (wejście w życie 2011 r)
- Nowelizacja ustawy o informatyzacji podmiotów realizujących zadania publiczne
- Informatyzacja postępowania cywilnego
- Dokument elektroniczny w postępowaniu administracyjnym oraz sądowym
- Zmiany w procedurze administracyjnej. Konsekwencje nowelizacji ustawy o informatyzacji na orzecznictwo sądów administracyjnych (seminarium dedykowane dla sądów administracyjnych)
- Zmiany w k.p.a. – konsekwencje dla urzędów ale także pełnomocników
- Konsekwencje zmian k.p.a. dla wydawania decyzji stypendialnych
- Zmiany w ordynacji podatkowej i k.p.a. Nowe obowiązki w związku z przesyłaniem dokumentów do Urzędu Skarbowego.
- Dostosowanie systemów teleinformatycznych urzędu oraz sądów do Krajowych Ram Interoperacyjności
- Nowa instrukcja kancelaryjna
- Umowy zawierane w działalności wydawniczej
- Odpowiedzialność aptekarza za błędne wydawanie leków
- Aktywności marketingowe w branży farmaceutycznej (aspekty prawne)
- Reklama wyrobów farmaceutycznych
- Problematyka pomocy prawnej
- Reklamacja w obrocie międzynarodowym. Regulacje UE, UNIDROIT i Konwencji wiedeńskiej
- Ochrona danych osobowych
- Faktura elektroniczna
- Umowy wdrożeniowe systemów IT
- Inne