présentant les avocats d'Europe
Representing Europe's lawyers
Reprezentujemy prawników
europejskich

KOMUNIKACJA ELEKTRONICZNA I INTERNET

KOMUNIKACJA ELEKTRONICZNA I INTERNET

Streszczenie

I. Zawartość poczty elektronicznej i stron internetowych

1. Dane

- Dane powinny być dokładne i aktualne.
- Należy stosować się do zasad wykonywania zawodu (podstawowy wymóg dotyczy zazwyczaj podawania nazwy i adresu firmy oraz danych wspólników lub informacji, gdzie takie informacje można uzyskać).

2. Charakter obsługi prawnej świadczonej on-line

- Należy wyjaśnić charakter udzielanej porady prawnej w celu uniknięcia nieporozumień i potencjalnych roszczeń przeciw prawnikom z tytułu niedokładnej lub niewłaściwej porady.

3. Linki i odniesienia do osób trzecich

- Należy zawsze zwracać uwagę, aby strony nie wydawały się zbyt obraźliwe dla zawodu lub niezgodne z podstawowymi zasadami wykonywania zawodu.

II. Korespondencja prawnika

1. Celowe przechwycenie i działania hakerów

- Należy rozważyć możliwości zastosowania i zapewnienia odpowiednich środków ochrony treści korespondencji przed jakąkolwiek oszukańczą modyfikacją takich jak np. podpisy elektroniczne lub szyfrowanie, lub obu tych środków: podpisy elektroniczne i szyfrowanie.
- Należy rozważyć możliwości zastosowania i zapewnienia środków komunikacji elektronicznej, w szczególności gdy korzysta się dostawców usług *webmail* (aplikacji internetowych pozwalających użytkownikom korzystać z usług poczty elektronicznej za pomocą przeglądarki internetowej), programów typu *online messenger* czy urządzeń mobilnych, które zapewniają rozsądny poziom ochrony przed przechwyceniem czy działaniami hakerów, które mogą skutkować ujawnieniem istnienia i treści komunikacji.
- Zawsze gdy poproszą o to klienci lub korespondenci należy stosować słusznie dostępne techniki szyfrowania.
- Gdy jest to konieczne, należy informować klientów i korespondentów o ryzyku związanym z korzystaniem z komunikacji elektronicznej.

2. Niezamierzony dostęp

- Należy ujmować w korespondencji ostrzeżenia dotyczące poufności.

3. Wirusy i złośliwe oprogramowanie

- Należy opracować strategię bezpieczeństwa i podstawowe procedury bezpieczeństwa.

4. Korespondencja elektroniczna pomiędzy prawnikami

- Należy pamiętać o zasadach wykonywania zawodu dotyczących wymiany korespondencji pomiędzy prawnikami za pomocą wiadomości elektronicznych.

III. Ochrona tajemnicy zawodowej i danych osobowych

- Proces przesyłania, odbierania i przechowywania korespondencji elektronicznej może obejmować proces przetwarzania danych osobowych, który wymaga stosowania odpowiednich środków ochrony danych w celu wywiązywania się z obowiązków zachowania tajemnicy zawodowej i stosowania się do innych właściwych przepisów prawa, i który musi być realizowany zgodnie z właściwymi przepisami prawa w zakresie ochrony danych.
- Należy wyświetlać informację dotyczącą poufności.

IV. Ochrona praw autorskich

- Należy weryfikować ochronę praw autorskich i stosować informacje dotyczące praw autorskich, gdy są one wymagane przepisami prawa.

V. Najlepsza praktyka

- Należy weryfikować tożsamość klienta on-line.
- Należy udzielać terminowych odpowiedzi klientom on-line.
- Należy przechowywać zapisy korespondencji elektronicznej.
- Należy utrzymywać standardy zachowywania i monitorowania prywatności użytkownika w zakresie korespondencji elektronicznej.
- Należy stosować się do zasad wykonywania zawodu dotyczących sporów transgranicznych prowadzonych w trybie on-line.

VI. Archiwizowanie dokumentów elektronicznych i wiadomości e-mail

- Należy opracować polityki dotyczące archiwizacji dokumentów elektronicznych i wiadomości e-mail, nie tylko w zakresie tego co powinno być archiwizowane, ale także w jaki sposób, w celu zapewnienia, że dokumenty elektroniczne i wiadomości elektroniczne będą dostępne w wymaganym okresie.
- Należy mieć świadomość, że zapisywanie dokumentów elektronicznych i wiadomości e-mail w jednym programie może mieć wpływ na możliwość ich wyszukania w stosownym czasie.
- Należy archiwizować dokumenty elektroniczne i wiadomości e-mail w zwyczajowo stosowanym formacie, zapewniając ich czytelność w przyszłości i ochronę oryginałów.

VII. Świadomość ukrytych danych w plikach i dokumentach

- Należy mieć świadomość, że pliki i dokumenty mogą zawierać ukryte dane, które nie są widoczne lub które dostarczają informacji o dokumencie i stanowią dane dodatkowe do głównej części tekstu (często zwane „metadanymi").
- Mogą istnieć metadane, których przechowywanie przez prawnika może okazać się użyteczne lub nawet niezbędne oraz inne dane, które prawnik musi usunąć w zależności od tego, dokąd są one wysyłane (np. plik prawnika, do klienta w celu wprowadzenia zmian w opcji zmian lub do prawnika dla osoby trzeciej).
- Ukryte dane mogą być powiązane z danymi widocznymi w taki sposób, że skopiowanie i przeklejenie danych widocznych skutkować będzie także przeniesieniem danych ukrytych.
- Zawsze należy sprawdzić czy w dokumentach elektronicznych stosowana jest funkcja „Śledź zmiany".
- Korzystając z funkcji „Śledź zmiany", należy upewnić się, że zmiany są widoczne i „zaakceptować" lub „odrzucić" zmiany przed wysłaniem dokumentu, o ile druga strona nie ma otrzymać dokumentu z widocznymi zmianami.
- Należy sprawdzić, że w pliku nie ma żadnej innej wersji dokumentu.
- Należy sprawdzić „Właściwości dokumentu" lub skorzystać z podobnej funkcji przed wysłaniem dokumentu, aby upewnić się, że nie zawiera on informacji nieprzeznaczonych dla odbiorcy.
- Należy korzystać z określonych programów, które umożliwiają analizę i usunięcie ukrytych danych.
- Należy rozważyć zainstalowanie systemu, który w sposób automatyczny sprawdza wysyłane dokumenty elektroniczne i wykasowuje ukryte dane.

KOMUNIKACJA ELEKTRONICZNA I INTERNET

Praktyczne wskazówki dla prawników
RADA ADWOKATUR I STOWARZYSZEŃ PRAWNICZYCH EUROPY

WPROWADZENIE

1. Świadcząc usługi prawnicze drogą elektroniczną, za pomocą poczty elektronicznej („poczta/wiadomość e-mail"), internetu czy dowolnych innych nowych technologii prawnicy mają możliwość poprawić jakość świadczonych przez nich usług oraz zwiększyć tempo ich świadczenia na rzecz klientów. Jednakże bez odpowiednich wskazówek, usługi elektroniczne mogą skutkować znaczącymi stratami, za które odpowiedzialność może ponosić kancelaria lub prawnik.

2. Jako narzędzie do komunikacji, wiadomość e-mail jest prosta w użyciu i wielu użytkowników traktuje ja bardziej jako ustny niż pisemny sposób przekazu. W konsekwencji, treść niektórych wiadomości elektronicznych może zostać równie dobrze odebrana jako oszczercza czy obraźliwa, gdy zostanie odczytana przez nieoczekiwanego odbiorcę. W takiej sytuacji, odpowiedzialność mogą ponosić zarówno prawnik wysyłający wiadomość, jak i zatrudniająca go kancelaria.

3. Strony (witryny) internetowe są coraz częściej wykorzystywane przez kancelarie prawne do celów reklamowych oraz do przekazywania porad prawnych czy informacji. Wielu prawników jest przekonanych, że świadcząc obsługę prawną w trybie on-line mają możliwość uzyskać dostęp do o wiele większej grupy klientów, zmniejszyć koszty stałe (prawnik nie potrzebuje już biura), zapewnić sobie elastyczny czas pracy i usprawnić procedury obsługi spraw za pomocą pobranych narzędzi internetowych takich jak oprogramowanie do zarządzania sprawami. Ale internet oznacza dla prawników także konkretne zagrożenia. Brak bezpośredniego kontaktu z klientem podczas spotkania może utrudnić prawnikowi dokonanie oceny sprawy i przekazanie pełnej porady; klient on-line może przyjąć tożsamość innej osoby (na przykład do celów testamentowych) a osoba może niewłaściwie przedstawiać siebie jako prawnika, które to sytuacje miały już miejsce w świecie realnym.

4. Archiwizowanie dokumentów elektronicznych i wiadomości e-mail stanowi kwestię istotnej wagi. Stosownie Rada Adwokatur i Stowarzyszeń Prawniczych Europy (dalej: Rada) uznała za konieczne zwrócenie krajowym Adwokaturom i Stowarzyszeniom Prawniczym uwagi na fakt, że elektroniczne i papierowe zapisy/rejestry muszą spełniać te same wymogi prawne w procesie ich przesyłania i archiwizowania. Rada zaleca przyjęcie polityk dotyczących archiwizowania dokumentów elektronicznych i wiadomości e-mai.

5. Aby móc czerpać korzyści z technologii on-line, minimalizując jednocześnie związane z nimi zagrożenia, kancelarie muszą zastanowić się w jaki sposób można przenieść standardy i najlepsze praktyki zawodu prawniczego do świata elektronicznego. Rada jest przekonana, że opracowanie polityki dotyczącej korzystania z internetu i poczty elektronicznej stanowi najlepszy środek do osiągnięcia tego celu.

6. W celu wsparcia stowarzyszeń prawniczych, adwokatur i kancelarii w procesie sporządzania ich własnych polityk, Rada opracowała wzorcową politykę korzystania z internetu i poczty elektronicznej. Polityka może wymagać dostosowania do zasad wykonywania zawodu w danym kraju i szczególnych okoliczności, w jakich działa dana kancelaria. Po jej przyjęciu, zaleca się przekazanie polityki wszystkim pracownikom kancelarii wraz ze stosowną informacją.

I. Zawartość poczty elektronicznej i stron internetowych

Prawnik i kancelaria mogą zostać pociągnięci do odpowiedzialności za błędne lub wprowadzające w błąd informacje, gdy udzielają porady lub przekazują informacje w formie elektronicznej lub papierowej. Toteż, należy zwracać uwagę na sprawdzanie danych pod kątem ich dokładności, aktualności i zgodności z zasadami wykonywania zawodu.

1. Dane: Stosowanie się do zasad wykonywania zawodu

a) Zasady:

Informacje, które muszą zostać zawarte w korespondencji prawnika mogą być różne w różnych krajach. Zasadniczo, wszystkie zasady wykonywania zawodu wymagają przekazywania podstawowych informacji, które pozwalają klientowi zweryfikować dane kancelarii i złożyć skargę na kancelarię. Dane te obejmują: nazwę i adres kancelarii, dane partnerów kancelarii lub informacje, gdzie takie informacje można uzyskać oraz wszelkie inne informacje dotyczące rejestracji usługodawcy zgodnie z Dyrektywą UE 2000/31/WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)[1].

b) Praktyczne wskazówki:

W zakresie stron internetowych kancelariom prawnym radzi się, aby informacje te były dobrze widoczne na ich stronie głównej.

W zakresie korespondencji elektronicznej, kancelarie prawne mogą chcieć wprowadzić szablony zgodnie z poniższym opisem.

Oprogramowanie do obsługi poczty elektronicznej może zapewniać użytkownikom jeden lub kilka standardowych szablonów zawierających informacje, które muszą oni podawać w swojej korespondencji.

Gdy kancelarie pozwalają użytkownikom wysyłać wiadomości prywatne, zaleca się, aby żądały one od prawników tworzenia wiadomości prywatnych za pomocą osobnego szablonu, który w jasny sposób wskazuje, że komunikacja pochodzi tylko od użytkownika a nie od kancelarii lub aby wymagały od prawników stosowania w komunikacji prywatnej innego wzoru podpisu.

Gdy kancelarie pozwalają użytkownikom uczestniczyć w publicznych dyskusjach na listach mejlingowych za pomocą wiadomości elektronicznych, ostrzeżenia dotyczące zachowania poufności lub tajemnicy nie są oczywiście właściwe, ale ich ujęcie może zmniejszyć wpływ takiej wiadomości. Kancelarie mogą chcieć także rozważyć przyjęcie do tych celów określonego szablonu.

2. Charakter obsługi prawnej świadczonej on-line

a) Zasady

Wiele osób, które kontaktują się z kancelarią prawną za pomocą strony internetowej lub poczty elektronicznej dysponuje niewielką lub żadną wiedzą prawniczą. Aby nie wprowadzić klienta w błąd, prawnik musi koniecznie w jasny sposób wyjaśnić klientowi, kiedy przekazywana przez niego komunikacja stanowi informację a kiedy poradę prawną.

Zasadniczo „informację" można zdefiniować jako materiał, który zawsze będzie taki sam niezależnie od osoby występującej o usługę prawną. Jeżeli jednak materiał zależy od osoby występującej o usługę, wtedy usługę tę należy zdefiniować jako „poradę".[2]

b) Praktyczne wskazówki:

W korespondencji elektronicznej prawnik będzie musiał wyjaśnić kiedy przekazana informacja stanowi poradę prawną a kiedy tylko informację. Kontekst korespondencji elektronicznej może pomóc w ustaleniu charakteru usługi.

---

[1] http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32000L0031&from=PL.

[2] Przykładowo: osoba zasięgająca informacji o stawce podatkowej we Francji w danym roku otrzyma informację. Jeżeli jednak osoba zasięga informacji o jej obowiązkach podatkowych w danym roku, wtedy otrzyma ona poradę.

W zakresie stron internetowych kancelariom radzi się, aby na stronie głównej wyraźnie zapisywały, że usługi świadczone przez stronę służą jedynie celom informacyjnym. Bez minimalnego kontaktu, nie ma możliwości udzielenia porady przez kancelarię; dlatego też wiele stron zawiera stwierdzenie, że poradę można otrzymać od prawnika za pomocą linka do wiadomości elektronicznej. Przykładową informacje prawną podano poniżej.

Przykładowa informacja prawna na stronie internetowej:

„Informacje podane na stronie internetowej stanowią wyłącznie informacje ogólne. Nie stanowią one ani porady prawnej ani żadnej innej profesjonalnej porady i nie powinny być jako takie wykorzystywane. Nasza kancelaria nie ponosi żadnej odpowiedzialności za działania podjęte na podstawie informacji zamieszczonych na naszej stronie."

3. Linki i odniesienia do osób trzecich

Gdy strona zawiera linki i odniesienia, użytkownik strony prawdopodobnie pomyśli, że kancelaria aprobuje usługi i informacje wskazane na stronach powiązanych. Należy zawsze zwracać uwagę, aby strony nie wydawały się zbyt obraźliwe dla zawodu lub niezgodne z podstawowymi zasadami wykonywania zawodu (np. gdy strona internetowa kancelarii prawnej zawiera reklamę lub link do towarzystwa ubezpieczeniowego, może to tworzyć wrażenie naruszenia niezależności).

II. Korespondencja prawnika

Zawodowa korespondencja prawnika z zasady stanowi korespondencję poufną. W celu ochrony korespondencji przed dostępem do niej osób nieupoważnionych Rada proponuje co następuje:

1. Celowe przechwycenie i działania hakerów

Prawnicy muszą chronić zawartość korespondencji elektronicznej przed jakąkolwiek oszukańczą modyfikacją, w szczególności w celu ochrony swoich własnych interesów.

W tym celu zaleca się, aby prawnicy stosowali słusznie dostępne środki komunikacji elektronicznej, które zapewniają integralność ich komunikacji elektronicznej.

Chociaż komunikacja elektroniczna jest technicznie i prawnie chroniona przed przechwyceniem przez osoby trzecie, poufność komunikacji może być narażona na różnorakie zagrożenia. Toteż prawnicy muszą ocenić ryzyko, na które narażona jest ich komunikacja elektroniczna (w szczególności gdy korzystają z dostawców usług *webmail*, programów typu *online messenger* lub urządzeń mobilnych) i zastosować odpowiednie środki np. skorzystać z technik szyfrowania danych stosownie do sytuacji, a także informować klientów i korespondentów o ryzyku, na które narażona jest komunikacja elektroniczna. Prawnicy nie powinni powstrzymywać się od stosowania słusznie dostępnego szyfrowania, zawsze gdy poproszą o jego zastosowanie klienci lub korespondenci.

2. Niezamierzony dostęp

Wiele kancelarii już zawiera ostrzeżenie dotyczące poufności w swoich wiadomościach faksowych, mając na względzie ryzyko ich błędnego przesłania do niewłaściwej osoby. Kancelarie powinny rozważyć zastosowanie podobnych ostrzeżeń dotyczących poufności w wiadomościach elektronicznych.

Automatyczne ostrzeżenia dotyczące poufności

Chociaż automatyczne ostrzeżenia dotyczące poufności prawdopodobnie nie skutkują żadnym wiążącym obowiązkiem prawnym dla nieoczekiwanego odbiorcy, oczekuje się, że wielu odbiorców zwróci na nie uwagę a ostrzeżenia mogą w ten sposób pomóc zapobiec szkodom, jakie mogą nastąpić wskutek błędu.

Poniżej podano przykładowe ostrzeżenie, które można odpowiednio dostosować: "Informacje zawarte w tej wiadomości stanowią informacje poufne. Wiadomość jest przeznaczona tylko dla jej adresata. Jeżeli nie są Państwo przewidywanym odbiorcą tej wiadomości prosimy o poinformowanie o tym fakcie nadawcy i natychmiastowe oraz całkowite usunięcie wiadomości z Państwa systemu."

Kancelarie mogą z pożytkiem dołączyć taką przykładową wiadomość z ostrzeżeniem do ich korespondencji elektronicznej wykorzystując w tym celu szablon lub wzór podpisu.

Kancelarie mogą być przekonane, że dołączanie takiego ostrzeżenia do całości korespondencji elektronicznej jest zbyt pracochłonne i mogą nie doceniać wagi takiego ostrzeżenia. Jednakże, o ile prawnicy nie zastanawiają się za każdym razem gdy wysyłają wiadomość czy powinni zawrzeć w niej to ostrzeżenie, zaleca się, aby takie ostrzeżenie było dołączane do każdej korespondencji elektronicznej.

Prawnicy muszą mieć na uwadze, że informacja prawnie chroniona w korespondencji prawnika może przestać być poufna, gdy wiadomość zostanie wysłana do innych osób (np. gdy wiadomość zostanie przez przypadek wysłana do adresów z listy mejlingowej)

3. Wirusy i złośliwe oprogramowanie

Korespondencja elektroniczna może zostać zawirusowana, co może mieć wpływ na stronę internetową i całą sieć kancelarii. Ponadto, wirusy i oprogramowanie tego typu mogą przekazywać informacje poufne lub zezwalać na nieuprawniony dostęp do tych informacji.

Kancelarie zachęca się, aby posiadały strategie bezpieczeństwa i stosowały aktualne środki techniczne zabezpieczające je przed takim ryzykiem. Kancelarie zachęca się także do zapewnienia, że użytkownicy pozostają czujni na znaczenie procedur bezpieczeństwa. Poniżej przedstawione zostały niektóre podstawowe procedury bezpieczeństwa.

(a) Wdrożenie oprogramowania antywirusowego.

(b) Konfiguracja serwerów poczty elektronicznej tak aby załączniki nie otwierały się automatycznie po otrzymaniu korespondencji. Zapewni to ochronę przez automatycznym zaimportowaniem wirusów do innych systemów.

(c) Zapewnienie, że sieć komputerowa kancelarii jest odpowiednio chroniona przed ingerencją czy wirusami z internetu.

Jeżeli kancelaria korzysta z internetu za pomocą stałego łącza, usilnie zaleca się zainstalowanie firewalli w celu zapewnienia ochrony systemów.

Jeżeli kancelaria korzysta z połączenia wdzwanianego, zaleca się rozważenie zainstalowania firewalla. Jeżeli koszty są zbyt wysokie, kancelaria powinna przynajmniej rozważyć odizolowanie komputerów, które mają dostęp do internetu od sieci kancelarii. W ten sposób zostanie zapewnione, że ingerencja lub wirus z internetu nie dotknie całej sieci kancelarii.

(d) Jeżeli sieć i komputery kancelarii są utrzymywane na podstawie umowy outsourcingu, zaleca się, aby kancelaria

- przeprowadzała odpowiednie kontrole bezpieczeństwa personelu wykonującego prace serwisowe i zapewniła, że personel posiada odpowiednie kwalifikacje techniczne;
- sprawowała odpowiedni nadzór nad wykonywanymi pracami;
- uzgadniała podejmowane działania pod kątem ich zgodności z zasadami dotyczącymi poufności i innymi zasadami etyki.

4. Korespondencja elektroniczna pomiędzy prawnikami

Przesyłając korespondencję drogą elektroniczną prawnicy muszą pamiętać o zasadach wykonywania zawodu, które na ogół mają zastosowanie do korespondencji prawniczej. Te zasady wykonywania zawodu mogą obejmować zasady dotyczące formy korespondencji, określonego okresu przechowywania, archiwizacji korespondencji czy zachowania jej poufności. Prawnicy, którzy wysyłają korespondencję drogą elektroniczną do prawnika w innym państwie członkowskim i którzy życzą sobie, aby pozostała ona poufna i nienaruszona powinni w jasny sposób zawrzeć tę intencję w przesyłanym dokumencie.

III. Ochrona tajemnicy adwokackiej i danych osobowych

Prawnicy powinni mieć świadomość, że proces przesyłania, odbierania i przechowywania korespondencji elektronicznej może obejmować proces przetwarzania danych osobowych, który wymaga posiadania odpowiednich środków ochrony danych w celu wywiązywania się z obowiązków zachowania tajemnicy zawodowej i stosowania się do innych właściwych przepisów prawa.

IV. Ochrona praw autorskich

Przed pobraniem pliku, prawnik powinien upewnić się, że nie naruszy w ten sposób praw autorskich.

Przykład informacji dotyczącej praw autorskich:

„Informacje podane na stronie internetowej podlegają ochronie z tytułu praw autorskich [© nazwa kancelarii]. Informacje nie mogą być kopiowane, ani w części ani w całości, ani w żadnej formie, o ile nie są one kopiowane w następującym celu:

1) Do użytku prywatnego

Informacje podane na stronie mogą być kopiowane, w części lub w całości, gdy przeznaczone są tylko do użytku prywatnego.

2) Do innych celów

Informacje podane na stronie mogą być kopiowane, w części lub w całości, na rzecz osoby trzeciej, pod warunkiem spełnienia następujących warunków:

a) skopiowane informacje wskazują tę stronę jako ich źródło i podają pełny adres strony oraz informację dotyczącą praw autorskich;

b) skopiowane informacje wskazują, że podlegają one ograniczeniom z tytułu praw autorskich, które osoba trzecia musi respektować;

c) skopiowane informacje nie mogą być wstawiane, ani w części ani w całości, do innego tekstu lub publikacji w żaden sposób bez uprzedniej zgody;

d) skopiowane informacje nie mogą być przechowywane, ani w części ani w całości, na innej stronie internetowej ani w innym systemie elektronicznym bez uprzedniej zgody;

e) skopiowane informacje nie mogą być przekazywane, ani w części ani w całości, do celów komercyjnych bez uprzedniej zgody.

Żadne informacje podane na tej stronie nie mogą być kopiowane, przesyłane czy przechowywane na innej stronie internetowej lub w innym systemie elektronicznym bez uprzedniej zgody, poza sytuacją gdy wykorzystuje się je do zindeksowania lub zaktualizowania jakichkolwiek wyszukiwarek internetowych czy podobnych usług mających na celu odesłanie użytkowników do tej strony."

Mogą mieć zastosowanie inne wyjątki zależnie od uwarunkowań lokalnych.

V. Zasady dotyczące najlepszych praktyk

Nie ma powodu, aby kancelarie nie podejmowały ani nie przyjmowały zobowiązań zawodowych drogą elektroniczną; jednakże kancelarie mogą chcieć zachować rozwagę, gdy akceptują takie zobowiązania w ten sposób.

Trudno jest wywnioskować na podstawie wyglądu wiadomości elektronicznej, że została ona naprawdę wysłana przez domniemanego nadawcę, chociaż jej kontekst może często na to wskazywać ponad wszelką wątpliwość.

Z czasem podpisy elektroniczne (ostatecznie w powiązaniu z danymi biometrycznymi) zapewnią o wiele lepszy dowód autentyczności wiadomości elektronicznej a stosowane na szeroką skalę techniki szyfrowania będą z dodatkową korzyścią dla lepszego procesu uwierzytelniania.

W międzyczasie, kancelariom przyjmującym zobowiązania zawodowe drogą elektroniczną zaleca się, aby sprawdzały czy kontekst zapewnia racjonalną pewność co do autentyczności wiadomości a w sytuacji jakichkolwiek wątpliwości sprawdzały telefonicznie lub faksowo, czy wiadomość taka pochodzi od domniemanego nadawcy.

Wiadomość e-mail: Automatyczne potwierdzenie odbioru: Kancelarie ostrzega się przed stosowaniem automatycznych potwierdzeń odbioru wiadomości e-mail. Ważne jest, aby prawnik wysyłał potwierdzenie tylko wtedy, gdy prośba o poradę lub informację została w pełni zrozumiana. Prawnik może chcieć poprosić klienta o dalsze informacje i ustalić z nim termin przekazania porady. Kancelarie powinny mieć świadomość, że może okazać się konieczne wyłączenie tej funkcji w opcjach programu poczty elektronicznej.

1. Znajomość Klienta

Kancelarie mogą przyjmować instrukcje drogą elektroniczną lub poprzez stronę internetową, jednakże powinny stosować w tym zakresie takie same kontrole i przeprowadzać taką samą analizę, jaką wykonują dla tradycyjnej komunikacji klienta z prawnikiem (komunikacja papierowa lub podczas bezpośrednich spotkań).

Potencjał internetu w zakresie anonimowych komunikacji może okazać się atrakcyjny dla oszustów finansowych i osób zajmujących się praniem pieniędzy a kancelarie muszą być czujne w zakresie ich obowiązków w tym obszarze.

Niektóre obszary działania takie jak sporządzanie testamentów czy postępowania rozwodowe rodzą

szczególne ryzyko, gdy działania te prowadzone są w sposób zdalny (na odległość). Jest to np. ryzyko podania się za kogoś innego czy wywierania niewłaściwego wpływu. Toteż wiadomości elektroniczne mogą skutkować wzrostem tego ryzyka i wymagać zachowania większej ostrożności.

2. Terminowa odpowiedź

a) Zasady:

Kancelarie już znają (lub powinny znać) zasady obsługi przychodzącej korespondencji listownej i faksowej oraz połączeń telefonicznych w sytuacji nieobecności przewidywanego odbiorcy.

Poczta elektroniczna przynosi nowe problemy, ponieważ może wpłynąć na skrzynkę niezauważona przez innych pracowników kancelarii. Kancelariom zaleca się poczynienie skutecznych technicznych i praktycznych ustaleń w celu zapewnienia, że na wiadomości elektroniczne odpowiada się w terminie i w odpowiedni sposób.

b) Praktyczne wskazówki:

Zaleca się, aby kancelarie stosowały odpowiedzi automatyczne podczas nieobecności zawsze wtedy, gdy pracownicy przebywają poza biurem przez jeden lub więcej dni, pod warunkiem że kancelarie zapewniają taką samą obsługę poczty elektronicznej, korespondencji listownej i faksowej podczas nieobecności prawnika. Ograniczona liczba osób (np. sekretarka i współpracownik) powinna mieć dostęp do skrzynki mejlowej prawnika pod jego nieobecność, w celu regularnego sprawdzania jej zawartości i zapewnienia, że wszelkie pilne zapytania są bezzwłocznie obsługiwane.

Systematyczne wysyłanie odpowiedzi automatycznych podczas nieobecności w odpowiedzi na każdą wiadomość elektroniczną może być zarówno denerwujące, jak i może dyskredytować kancelarię, zwłaszcza gdy nieobecny prawnik zapisał się na listy mejlingowe i subskrypcja ta jest kontynuowana pod jego nieobecność. Aby uniknąć takiej sytuacji zaleca się, aby kancelarie – gdy tylko mają taką możliwość – ustawiały odpowiedzi automatyczne podczas nieobecności w taki sposób, aby były one wysyłane do każdego nadawcy tylko raz.

3. Spam

Masowe reklamy i oferty przesyłane drogą elektroniczną, które zazwyczaj określa się terminem „spam" mogą stanowić istotny problem dla kancelarii korzystających z poczty elektronicznej. Dostępne jest oprogramowanie filtrujące służące do ograniczenia liczby wiadomości będących spamem. Jednakże w sytuacji gdy kancelarie stosują filtry spamu powinny one uprzedzić o tym klientów, aby uniknąć zablokowania uzasadnionej korespondencji. Powinny wyjaśnić, że po wysłaniu ważnej informacji należy zawsze zatelefonować lub wysłać faks, lub też przesłać wydruk wiadomości tradycyjną pocztą. Kancelarie, które same obsługują swoje serwisy pocztowe powinny rozważyć odsyłanie korespondencji reklamowej/ofertowej do nadawcy wraz z określoną wiadomością.

4. Zapisy/rejestry

Tak jak dokumentacja papierowa jest przechowywana w celu zachowania kopii poczty wychodzącej i notatek z rozmów telefonicznych, tak samo kopie wiadomości elektronicznych (inne niż te, które nie są ważne z punktu widzenia prawa) powinny być przechowywane w pliku. Jeżeli chodzi o autentyczność, należy także rejestrować metadane z wiadomości elektronicznych. Obecnie zaleca się korzystanie z dokumentacji papierowej, choć podejście to może ulec zmianie, gdy pojawią się prawdziwie elektroniczne biura.

Prawnicy powinni mieć świadomość, że skasowana wiadomość elektroniczna może zostać odzyskana. W sporach nawet skasowane wiadomości elektroniczne mogą podlegać ujawnieniu.

Szczegółowe wskazówki podano w ust. VI.

5. Prywatność użytkownika

a) Zasady:

Kancelarie muszą monitorować korespondencję i komunikację swoich prawników i pozostałych pracowników w celu zapewnienia zachowywania przez nich ich standardów zawodowych. W sytuacji gdy porada jest przekazywana przez pracownika drogą elektroniczną, kancelarie muszą być w stanie sprawdzić trafność tej porady.

Zazwyczaj dokonuje się tego w trakcie przeglądu dokumentacji papierowej, ale może się zdarzyć, że kancelarie będą chciały sprawdzać wiadomości wychodzące i przychodzące pracownika.

Gdy dopuszcza się wykorzystywanie systemu kancelarii do obsługi poczty prywatnej, taka kontrola może stanowić naruszenie prywatności pracowników kancelarii. W niektórych jurysdykcjach, takie kontrole mogą być bezprawne.

b) Praktyczne wskazówki dla prawników korzystających z poczty elektronicznej:

Jeżeli użytkownikom pozwolono wysyłać wiadomości prywatne z systemu kancelarii, ich izolacja od innych wiadomości elektronicznych do celów monitorowania może okazać się nieuzasadniona.

Zgoda pracownika na monitorowanie korespondencji powinna stanowić element warunków zatrudnienia w kancelarii a możliwość dokonania takiej czynności powinna zostać jasno wskazana.

6. Korespondencja transgraniczna w trybie on-line: zasady wykonywania zawodu

Jeżeli prawnik świadczy usługi drogą elektroniczną, zasady, którym podlega relacja prawnika z klientem zależą od miejsca świadczenia usług przez prawnika[3]:

Przykładowo:

- Irlandzki prawnik udziela porady drogą elektroniczną klientowi w Belgii.
- Zgodnie z Dyrektywą o handlu elektronicznym relacja prawnika z klientem podlega zasadom wykonywania zawodu w Irlandii.

Jeżeli prawnik świadczy usługi drogą elektroniczną na rzecz klienta spoza UE, zaleca się, aby obie strony uzgodniły zasady mające zastosowanie do ich relacji.

VI. Archiwizowanie dokumentów elektronicznych i wiadomości e-mail

Technologie informacyjne rozwijają się szybko i coraz częściej nie przechowuje się kopii papierowej każdego dokumentu, jednakże z perspektywy prawnej konieczne jest archiwizowanie określonych dokumentów i wiadomości e-mail przez kilka lat. Jak wskazano powyżej, prawnicy powinni mieć świadomość, że w sporach nawet skasowane wiadomości elektroniczne mogą podlegać ujawnieniu.

1. Archiwizowanie wiadomości e-mail

Wiadomość e-mail stanowi znakomity przykład dystrybuowanej komunikacji, która jest przez to trudna do kontrolowania. Wiele osób jest przekonanych, że wiadomość e-mail nie posiada oficjalnego statusu. Pracownicy często sami decydują co powinno a co nie powinno być przechowywane i zapisują lub kasują wiadomości elektroniczne według własnego uznania, ponieważ pozostają w błędnym przekonaniu, że poczta elektroniczna stanowi część ich własnej prywatnej domeny roboczej. Kancelarie muszą posiadać stałe polityki wskazujące, które wiadomości elektroniczne muszą być przechowywane. Z zasady, stosuje się te same kryteria jak do „zwykłej" poczty papierowej. Wymogi określone prawem dla dokumentów papierowych będą miały także zastosowanie do dokumentów elektronicznych. Format dokumentu nie jest ważny. Powinny istnieć także wytyczne dotyczące wykorzystywania i organizowania wiadomości elektronicznych, ponieważ ludzie mają w zwyczaju je drukować i stąd nie są one przechowywane we właściwy sposób. W ten sposób traci się część kontekstu lub inne informacje, przez co zmniejsza się ich dostępność.

2. Podpis elektroniczny[4]

Ze względu na coraz szersze stosowanie podpisów elektronicznych w dokumentach i wiadomościach elektronicznych, kwestia zachowania podpisów także wysuwa się na pierwszy plan. Niektóre dane, na których bazują podpisy elektroniczne i które w dużym stopniu determinują zaufanie pokładane w podpisie elektronicznym są przechowane przez akredytowane podmioty świadczące usługi certyfikacyjne w rozumieniu Dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych. Dane te obejmują głównie dane, które stanowią dowód autentycznej certyfikacji (wykorzystane do certyfikacji dane pochodzące z dokumentów tożsamości, formularzy wniosków i podpisanych warunków) i dane historyczne dotyczące anulowanych certyfikatów. Dane mogą okazać się bardzo ważne w sytuacji sporu

---

[3] Dyrektywa UE 2000/31/WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym): http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32000L0031&from=PL.

[4] Zob. także Dyrektywa 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych, Dz.U. L13 z dnia 19 stycznia 2000, str. 12.

dotyczącego autentyczności czy stosowalności podpisu elektronicznego.

3. Autentyczność

Ważne jest także, aby zachować cechy charakterystyczne dokumentu elektronicznego w celu zapewnienia ochrony jego integralności. Można to osiągnąć w dużej mierze poprzez opracowanie strategii, w której zapisać można ważne aspekty treści, struktury, wyglądu i zachowywania dokumentu. Zachowanie cech charakterystycznych archiwizowanych dokumentów elektronicznych jest bardzo ważne. W końcu ważny element stanowi także uwierzytelnienie. Kontekst sporządzenia i wykorzystania dokumentu oraz wszelkie zmiany poczynione w wyniku działań zarządzania czy zachowywania dokumentu są opisane w metadanych[5]. To umożliwia wykazanie czy zweryfikowanie stopnia autentyczności tworzonego i obecnie wykorzystywanego zarchiwizowanego dokumentu.

Gdy dokument elektroniczny zostaje odtworzony na innym środowisku komputerowym niż jego środowisko oryginalne, może on całkiem inaczej wyglądać i całkiem inaczej się zachowywać. Jeżeli przeniesienie na inne środowisko komputerowe nie podlega kontroli, może zostać naruszona autentyczność dokumentu elektronicznego. Autentyczność stanowi kluczowe pojęcie w zachowywaniu dokumentów w sposób elektroniczny lub inaczej. Autentyczność określa, że dokument jest tym za jaki się podaje i że został sporządzony przez określoną osobę. Autentyczność dokumentów może być chroniona poprzez opisanie i zachowanie oryginalnego kontekstu dokumentów i utrzymanie nienaruszonego łańcucha jego przechowywania. Integralność dokumentu zostaje zachowana, gdy jest on kompletny i gdy nie zostały zakłócone jego zasadnicze aspekty; tzn. dokument nie został naruszony, zmieniony czy uszkodzony w taki sposób, że jego znaczenie przestało być jasne. Dopuszcza się zmiany w określonym zakresie, o ile nie zmieniają one oryginalnego znaczenia czy funkcji dokumentu.

W zasadzie nie ma różnicy czy dokument jest w formie elektronicznej czy fizycznej: zawsze należy zapewnić autentyczne zachowanie dokumentu. Jednak problem, który dotyczy dokumentów elektronicznych polega na tym, że ze względu na zmieniającą się technologię nie wszystkie aspekty dokumentu mogą zostać zachowane tak dokładnie jak w chwili jego sporządzenia. Nie oznacza to jednak, że trwałe zachowanie autentycznych dokumentów elektronicznych nie jest możliwe.

Tak jak wspomniano powyżej, archiwizowanie dokumentów elektronicznych i wiadomości e-mail różni się od archiwizacji dokumentów papierowych. O ile w chwili tworzenia dokumentu lub wiadomości e-mail uwzględni się poniższe punkty, łatwiej będzie później zarchiwizować dokumenty i wiadomości e-mail, które ze względu na wymogi prawne muszą być przechowywane przez kilka lat.

a) Dokument

O ile uwzględni się poniższe punkty, łatwiej będzie później zarchiwizować[6] dokumenty:

- do tworzenia dokumentów należy stosować szablony[7];
- należy zacząć tworzyć dokumenty za pomocą pustego szablonu, w przeciwnym razie informacje (metadane[8]) z innych dokumentów mogą zostać zawarte w nowym dokumencie i będą zawierały błędne informacje
- należy sprawdzić czy informacja na ekranie właściwości[9] jest aktualna;
- należy poinstruować użytkowników, aby stosowali jasną strukturę dokumentów, tzn. profile i nagłówki;
- należy kopiować i wklejać tak mało informacji jak to tylko możliwe w celu przeciwdziałania ujęciu w dokumencie nieprawidłowych metadanych;
- nie należy stosować haseł do zabezpieczania dokumentów, ponieważ w sytuacji utraty

[5] Nie tylko sam tekst dokumentu zawiera ważne dane; metadane też są ważne. Metadane to dane o danych. Metadane są dodawane do dokumentu elektronicznego w celu opisania dodatkowych informacji z zakresu pięciu cech charakterystycznych dokumentu wskazanych powyżej tak aby móc np. sprawdzić czy dokument jest tym za jaki się „podaje". Jednocześnie, metadane umożliwiają pozyskanie i wykorzystanie danego dokumentu elektronicznego. Przykładowe metadane to domniemany autor dokumentu, przedmiot, proces biznesowy, w którym dokument został utworzony czy data utworzenia dokumentu. Ale metadane są także ważne w kontekście rejestrowania wykonania działań służących zachowaniu dokumentu.
[6] Zob. ustęp dotyczący archiwizacji.
[7] Szablon zawiera modelowy układ dokumentów.
[8] Zob. w 4.
[9] Ta opcja zazwyczaj znajduje się pod nagłówkiem „pliku" twojego programu do tworzenia dokumentów typu word. Zawiera ona np. informację kiedy dokument został utworzony i przez kogo oraz czy dokument podlegał zmianom.

hasła dokumentu nie da się otworzyć; lepiej jest stosować zamiast hasła opcję tylko do odczytu;

- należy stosować standardowe czcionki np. Arial, Times New Roman, ponieważ są one rozpoznawane przez inne programy;
- należy stosować nagłówki i stopki do wstawiania metadanych takich jak nazwa i numer wersji dokumentu;
- nie należy stosować automatycznych pól dnia i godziny, ponieważ mogą one ulegać zmianie przy każdym otwarciu dokumentu;
- należy stosować tabele lub tabulatory, gdy jest taka konieczność i unikać spacji, tak aby zachować stały układ dokumentu;
- należy zapisywać dokument centralnie na serwerze a nie na dysku twardym stacji roboczej, tak aby każdy miał dostęp do najnowszej wersji dokumentu.

b) Wiadomość e-mail

Aby móc zdecydować czy wiadomość e-mail musi zostać zarchiwizowana, można dokonać rozróżnienia bazując na poniższych komentarzach.

aa) Adresowanie wiadomości elektronicznych

- zawsze należy korzystać z książki adresowej, ponieważ zawiera ona dodatkowe informacje o osobach, do których wysyła się wiadomość;
- należy zachować ostrożność podczas korzystania z list dystrybucyjnych, ponieważ mogą one często ulegać zmianie a kiedy zmiana ma miejsce, brak jest informacji w tym zakresie i można nie zauważyć do kogo wiadomość e-mail została pierwotnie wysłana;
- nawet jeżeli wydaje się to oczywiste: zawsze należy wpisywać temat wiadomości e-mail; pomaga to w ocenie wiadomości;
- należy korzystać z opcji wiadomości takich jak „wysoka ważność” tylko wtedy, gdy jest absolutnie konieczne, ponieważ nie wszystkie aplikacje poczty elektronicznej są w stanie odtworzyć takie informacje w prawidłowy sposób;

bb) Sporządzanie wiadomości e-mail

- gdy tylko jest to możliwe, należy sporządzać i wysyłać wiadomości z wykorzystaniem zwykłego tekstu lub formatu html, ponieważ nie wszystkie programy poczty elektronicznej są w stanie odczytać różne czcionki
- nie należy stosować wiadomości z automatycznie aktualizującymi się polami (są one niestabilne i mogą aktualizować się przy każdym otwarciu wiadomości e-mail)
- należy rozsądnie podchodzić do załączników (przesyłać obrazy w formacie mapy bitowej lub .jpeg a nie wklejone do innej aplikacji)
- odpowiadając na wiadomość e-mail nie należy „wstawiać”, ale wpisać swoje komentarze powyżej oryginalnej wiadomości i należy zostawić miejsce pomiędzy nagłówkami oryginalnej wiadomości a swoim podpisem
- należy korzystać ze wzoru podpisu zawierającego ważne informacje kontekstowe, tak aby łatwiej było namierzyć nadawcę

cc) Zarządzanie wiadomościami e-mail

- należy zapewnić, że skrzynka odbiorcza jest dobrze zarządzana; kiedy odbiera się wiadomość, należy zdecydować czy musi ona zostać zachowana i jeżeli tak przenieść ją do odpowiedniego folderu
- jeżeli nie posiada się specjalnego systemu do przechowywania wiadomości, należy utworzyć katalogi dla wiadomości e-mail, które muszą zostać zachowane tak aby ułatwić ich znalezienie i należy upewnić się, że wiadomość przychodzące i wychodzące są przechowywane w tym samym katalogu
- nigdy nie należy wklejać treści wiadomości do innej aplikacji i kasować oryginalnej

wiadomości, ponieważ może to poważnie zaszkodzić autentyczności i integralności dokumentu (metadane[10] zostaną utracone)

dd) Poczta przychodząca i wychodząca (wewnętrzna i zewnętrzna)

To rozróżnienie jest innego rodzaju, niż klasyfikacje podane poniżej, jednakże dotyczy regulacji w zakresie obsługi poczty elektronicznej. Rozróżnienie pomiędzy wewnętrzną i zewnętrzną wiadomością e-mail także można poczynić w tej kategorii, rozróżniając pomiędzy wiadomościami elektronicznymi wymienianymi w ramach organizacji i wiadomościami wymienianymi z osobami spoza organizacji.

ee) Korespondencja służbowa a korespondencja prywatna

Wiadomość e-mail wysyłana lub odbierana przez pracownika stanowi część jego poczty służbowej. Wiadomość e-mail wysyłana lub odbierana przez osobę prywatną, która nie dotyczy faktu zatrudnienia pracownika w organizacji jest klasyfikowana jako wiadomość prywatna.

ff) Wiadomość e-mail do zachowania a wiadomość e-mail do usunięcia

Gdy wiadomość e-mail ma jakąś funkcję do spełnienia, należy podjąć decyzję odnośnie do konieczności jej zachowania. Z zasady, także tutaj stosuje się takie same kryteria jak do „zwykłej" poczty papierowej.

c) Archiwizowanie dokumentów elektronicznych i wiadomości e-mail

Radzi się, aby zachowywać wersje oryginalne dokumentów i wiadomości elektronicznych za pomocą programu, w którym były przygotowywane, ponieważ nie wiadomo, co programy mogą zrobić w przyszłości ze „starymi" (elektronicznie zarchiwizowanymi) wersjami dokumentów i wiadomości elektronicznych. Zaleca się także korzystanie ze zwyczajowo stosowanego formatu i stosowanie tego samego formatu do wszystkich dokumentów i wiadomości elektronicznych. Podczas archiwizowania dokumentów i wiadomości elektronicznych należy pamiętać, że ważne jest zarówno zachowanie czytelności dokumentu w przyszłości, jak i ochrona oryginalnych wersji dokumentów i wiadomości elektronicznych.

VII. Świadomość ukrytych danych w plikach i dokumentach

Ważne jest, aby mieć świadomość, że dokumenty elektroniczne i inne pliki komputerowe często zawierają dodatkowe informacje, które dostarczają informacji o dokumencie lub o jego domniemanym autorze i że dane te mogą być dostępne lub ukryte, np. autor, data i godzina utworzenia i ostatniej zmiany, wykorzystany szablon itp. W zależności od charakteru informacji i kontekstu, w którym później się pojawia, informacja może okazać się przydatna, nieszkodliwa lub wprawiająca w zakłopotanie, potencjalnie niebezpieczna lub też może skutkować przypadkowym ujawnieniem informacji poufnej lub informacji nieprzeznaczonej dla odbiorcy dokumentu. Z drugiej strony przechowywanie takich danych może także okazać się przydatne lub nawet niezbędne dla prawnika. W takiej sytuacji, prawnik będzie musiał podjąć kroki w celu zachowania metadanych i nieprzekazania ich osobom trzecim.

a) Ponowne wykorzystanie dokumentu i ujawnienie informacji

Prawnicy są ekspertami w ponownym wykorzystywaniu dokumentów; jest bardzo rozpowszechnioną praktyką wykorzystywanie dokumentu jako punktu wyjścia przy tworzeniu innego dokumentu w innej sprawie dla innego klienta i nowego dokumentu jako punktu wyjścia w jeszcze kolejnej sprawie dla jeszcze innego klienta. Jeżeli prawnik nie ma świadomości istnienia ukrytych danych, może się zdarzyć, że odbiorca ostatniej wersji dokumentu, analizując ukryte dane będzie w stanie stwierdzić dla kogo utworzono oryginalny dokument i jakie zmiany czy poprawki zostały wprowadzone do dokumentu przez różne osoby go przeglądające. Kopiowanie i wklejanie treści dokumentu do nowego dokumentu nie stanowi wiarygodnej metody unikania przenoszenia ukrytych danych, ponieważ niektóre ukryte dane są powiązane z tekstem w taki sposób, że przeklejenie tekstu do nowego dokumentu skopiuje także oryginalne ukryte dane.

b) Wersjonowanie

Funkcja „Śledź zmiany" w programie Microsoft Word pozwala zobaczyć zmiany wprowadzone w kolejnych wersjach dokumentu; jednakże z funkcji tej należy korzystać z rozwagą. Funkcja „Śledź

[10] Zob. w 4.

zmiany” może być włączona, ale użytkownik może mieć tę funkcję nieaktywną, w wyniku czego zmiany wprowadzone do dokumentu oraz autorów zmian będzie można zobaczyć po ponownym aktywowaniu tej funkcji.

Jako ogólną wskazówkę sugeruje się, aby użytkownicy zawsze sprawdzali czy funkcja „Śledź zmiany” jest stosowana czy też nie. Jedynym sposobem pozbycia się zapisanych zmian w kolejnych wersjach dokumentu jest ich akceptacja lub odrzucenie.

c) Wykorzystywanie dokumentów PDF zamiast dokumentów w formacie Microsoft Word do dystrybucji dokumentów

Dokumenty w formacie PDF stanowią dobrą alternatywę dla dokumentów w programie Microsoft Word. W większości przypadków plik PDF jest odporny na kwestie wskazane powyżej, ponieważ dokumenty w formacie PDF tylko pokazują dokument w formie w jakiej zostanie on wydrukowany. Należy jednak zwrócić uwagę, że np. wstawienie czarnego lub białego pola nad tekstem nie usunie tekstu, ale umieści pole nad tekstem i stosownie ukryje tekst podczas wydruku. Skasowanie pola ponownie odkryje tekst. Dokumenty PDF obsługują wiele ukrytych danych dotyczących użytkownika, ale w praktyce wykorzystanie tych danych jest prawie niespotykane. Jednakże, aby mieć pewność, zaleca się sprawdzenie „Właściwości dokumentu” przed jego dystrybucją.

Należy odnotować, że istnieją różne rodzaje formatów PDF. Dokument PDF utworzony poprzez zeskanowanie tekstu za pomocą skanera czy drukarki może zawierać tylko obraz znaków na kartce papieru. Tekst w takim dokumencie nie może zostać wyszukany za pomocą narzędzi wyszukiwania i nie da się go w prosty sposób skopiować i wkleić do innych dokumentów. Z drugiej strony dokument PDF zapisany z programu do tworzenia dokumentów typu word zazwyczaj zostaje zapisany jako tekst a nie zwykły obrazek. Dokumenty w tej formie wymagają mniej miejsca do przechowywania niż dokumenty PDF. Z tych powodów, dokumenty powinny zazwyczaj być zapisywane jako tekstowe dokumenty PDF (a nie obrazy PDF), gdy mają być przechowywane w możliwych do przeszukania bazach danych lub gdy ważne jest ograniczenie ich rozmiaru (np. jako załączniki do wiadomości elektronicznych).

d) Specjalne narzędzia do kasowania ukrytych danych

Istnieją specjalne narzędzia komputerowe (programy), które analizują dokumenty i kasują stare zapisy lub ukryte dane. Zaleca się zainstalowanie i korzystanie z takich narzędzi przed dystrybucją informacji wrażliwych w dokumentach elektronicznych. Narzędzia te można pobrać np. ze strony firmy Microsoft i zainstalować w wersji Office2003/XP. Wersja Word Office 7 posiada domyślne **narzędzie** (zob. „przycisk pakietu Office”/”Sprawdź dokument”).