Pytania i odpowiedzi
dotyczące ochrony danych osobowych
w kancelariach prawnych

1. Czy przetwarzanie danych osobowych w kancelariach prawnych podlega ustawie o ochronie danych osobowych?

Przedmiotem regulacji ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2015 r., poz. 2135) (dalej: „Ustawa"), zgodnie z art. 2 ust. 1 Ustawy objęte są „zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych". Art. 3 ust. 2 pkt 2 Ustawy stanowi zaś, iż Ustawę stosuje się do osób fizycznych i osób prawnych oraz jednostek organizacyjnych niebędących osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych. Z opisanego przedmiotu regulacji wynika więc jednoznacznie, że przetwarzanie danych przez radców prawnych w związku z prowadzoną przez nich działalnością zawodową podlega przepisom uregulowanym w Ustawie o ochronie danych osobowych.

2. Na czym polega zatem zwolnienie opisane w art. 43 ust. 2 pkt 5 Ustawy?

Art. 43 ust. 2 pkt 5 Ustawy zwalnia radców prawnych jedynie z **obowiązku rejestracyjnego zbiorów danych do GIODO** i to tylko tych, które przetwarzane są w związku ze świadczeniem pomocy prawnej. Tym samym wyłączeniu nie podlegają np. zbiory danych zebrane w celach marketingowych. Ponadto, wyłączenie nie powinno powodować mylnego przekonania, że na kancelariach nie spoczywają inne obowiązki wynikające z Ustawy – w tym w szczególności obowiązki związane z zapewnieniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych oraz prowadzeniem właściwej dokumentacji (art. 36 Ustawy). Ten obowiązek spoczywa bezwzględnie na każdym podmiocie przetwarzającym jakiekolwiek dane osobowe z jakiegokolwiek tytułu.

3. Czy kancelaria prawna (w tym jednoosobowa) jest administratorem danych w świetle przepisów Ustawy?

W rozumieniu przepisu art. 7 pkt 4 Ustawy kancelaria prawna (również jednoosobowa) jest administratorem danych. Za administratora uważa się bowiem organ, jednostkę organizacyjną, podmiot lub osobę decydującą o celach i środkach przetwarzania danych, pod warunkiem, że dane są przetwarzane w związku z prowadzoną działalnością zarobkową, zawodową lub dla realizacji celów statutowych. Ustawa nie przewiduje wyjątków w tym zakresie. Stosowanie ustawy będzie jednak odpowiednio ograniczone w odniesieniu do danych i informacji podlegających ochronie wynikającej z przepisów szczególnych, w tym dotyczących tajemnicy zawodowej radców prawnych. Należy jednak podkreślić, że:

1) Działanie ustawy nie będzie ograniczone w całości, a jedynie w stosunku do aspektów, które zostały odrębnie uregulowane w sposób zapewniający dalej idącą ochronę, niż wynikałoby to z zastosowania ustawy – np. dostępu samego organu kontrolnego – GIODO – do zbiorów danych objętych tajemnicą zawodową.
2) Ustawa będzie miała zastosowanie w całości w stosunku do danych, które są przetwarzane w kancelarii, a które nie podlegają tajemnicy zawodowej.
3) Obowiązki stosowania środków organizacyjnych i technicznych zapewniających ochronę tym danym stosuje się bezwzględnie do wszystkich danych osobowych przetwarzanych przez administratora.

4. Jakie rodzaje/kategorie danych osobowych są przetwarzane w kancelarii prawnej?

Kancelaria prawna, w toku prowadzonej działalności zawodowej przetwarza różnego rodzaju dane osobowe, w stosunku do których nie można zastosować wyłączenia działania ustawy. Przykładowo, kancelaria prawna będzie zapewne przetwarzać dane osobowe następujących kategorii:

1) Dane przetwarzane w związku z zatrudnieniem:
    a. Dane kandydatów do pracy, pracowników, współpracowników, zleceniobiorców.
2) Dane dostawców usług oraz osób świadczących usługi:

   a. Dane dostawców, usługodawców, dane osób wspierających działania kancelarii w formie np. praktyk, staży, itp.
3) Dane klientów:
   a. Dane klientów, które przetwarzane są w celu wystawienia rachunku, faktury i prowadzenia rozliczeń finansowych
   b. Dane obecnych i byłych klientów – w zakresie ograniczonym do danych niezbędnych do identyfikacji oraz wskazania charakteru współpracy przetwarzane w celu bieżącej organizacji oraz badań rynku.
   c. Dane potencjalnych klientów – w podstawowym zakresie niezbędnym do prowadzenia planowania rozwoju działalności oraz analiz rynku.

5. Jakie dane są chronione ustawą? Co to są dane osobowe?

Za dane osobowe w rozumieniu art. 6 Ustawy uznaje się wszelkie informacje, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zatem, o ile dany zestaw informacji będzie umożliwiał bezpośrednią, bądź pośrednią identyfikację danej osoby, powinien być traktowany jako zawierający dane osobowe. O tym, czy dana informacja przejawia charakter osobowy przesądza zatem nie przynależność tej informacji do odpowiedniej kategorii, tylko kontekst, w jakim jest ona wykorzystywana oraz czy pozwala na zidentyfikowanie osoby.

6. Jakie są podstawowe obowiązki kancelarii jako administratora danych?

Ustawa o ochronie danych osobowych określa szereg obowiązków spoczywających na administratorze danych. Przede wszystkim jednak kancelaria powinna:

1) przetwarzać dane zgodnie z prawem, czyli nadzorować, aby pozyskiwane były wyłącznie te dane, których gromadzenie nie jest zabronione oraz w sposób, który zapewni respektowanie praw osób, których dane dotyczą. Poprzez legalne przetwarzanie danych rozumie się również wypełnianie wszelkich obowiązków administracyjnych spoczywających na administratorach danych, takich jak zgłoszenie zbiorów do rejestracji w GIODO, wystąpienie do GIODO o zgodę lub wydanie decyzji, prowadzenie dokumentacji zgodnie z przepisami, itp.,
2) gromadzić wyłącznie te dane, które są niezbędne do osiągnięcia celu przetwarzania i powstrzymać się od gromadzenia nadmiernych danych na temat osób, których dane dotyczą,
3) przetwarzać dane wyłącznie w określonym, zgodnym z prawem celu – powstrzymać się od gromadzenia danych „na zapas”,
4) przechowywać dane wyłącznie w czasie, jaki jest niezbędny do realizacji celu przetwarzania, a po tym czasie – bezpiecznie usunąć dane,
5) dbać o jakość danych, aby były one zgodne z prawdą również poprzez usuwanie danych błędnych lub nieprawdziwych,
6) przetwarzać dane w taki sposób, aby osoba, której dane dotyczą w łatwy sposób mogła zasięgnąć informacji na temat przetwarzania danych na jej temat oraz miała możliwość skorzystania z przysługujących jej praw,
7) zabezpieczyć przetwarzanie danych w taki sposób, aby zapewnić poufność, integralność i dostępność danych. Poziom oraz rodzaje zabezpieczeń powinny być każdorazowo oceniane i dostosowywane przez administratora danych, zależnie od okoliczności w jakich dane są przetwarzane.

7. Jak przygotować dokumentację przetwarzania danych osobowych?

Jednym z wymagań spoczywającym na administratorach danych jest prowadzenie dokumentacji przetwarzania i ochrony danych. Dokumentacja powinna określać jakie dane są przetwarzane w kancelarii, w jaki sposób należy chronić te dane oraz systemy informatyczne. Rozporządzenie z dnia 22 kwietnia 2004 r. w sprawie dokumentacji

przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) definiuje podstawowy zakres dokumentacji jaka powinna być prowadzona. Zgodnie z rozporządzeniem każdy administrator danych zobowiązany jest prowadzić:

1) politykę bezpieczeństwa, która powinna opisywać zasady przetwarzania danych osobowych, określać, jakie dane są przetwarzane w kancelarii, oraz jak są one zabezpieczone. W tym dokumencie należy wskazać środki techniczne i organizacyjne, które powinny zostać zastosowane i które administrator danych wdrożył do stosowania, aby osiągnąć bezpieczeństwo przetwarzania danych osobowych.
2) instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, która określa minimalne wymagania, jakie powinny spełniać systemy informatyczne oraz osoby, nadzorujące, czy też wspierające te systemy, aby zapewnić bezpieczeństwo przetwarzania danych z wykorzystaniem tych systemów.

Dodatkowo, administrator danych zobowiązany jest dopuścić do przetwarzania danych wyłącznie osoby do tego upoważnione oraz, zgodnie z art. 39 ustawy, prowadzić ewidencję tych osób w taki sposób, aby możliwe było wskazanie kto, kiedy i w jakim zakresie posiada (lub posiadał) dostęp do danych osobowych.

8. Czy kancelaria prawna musi powołać administratora bezpieczeństwa informacji?

Administrator bezpieczeństwa informacji (ABI), czyli osoba odpowiedzialna za nadzór nad przetwarzaniem danych osobowych u administratora danych może zostać powołany, lecz nie jest to bezwzględnym obowiązkiem. Zgodnie z Ustawą, od 1 stycznia 2015 r. w przypadku powołania ABI administrator danych zwolniony jest z pewnych obowiązków związanych z rejestracją zbiorów danych osobowych. Powołanie ABI należy w ciągu 30 dni zgłosić do GIODO. Na ABI zgłoszonym w GIODO ciąży szereg obowiązków określonych w art. 36a Ustawy. W przypadku niepowołania ABI obowiązki określone w tym przepisie spoczywają na administratorze danych. Wyznaczenie ABI powinno docelowo zapewniać podwyższenie poziomu bezpieczeństwa przetwarzania danych osobowych. Osobą powołaną może być jedynie osoba fizyczna i nie może być to administrator danych.

9. Czy GIODO ma uprawnienia do przeprowadzenia kontroli w kancelarii?

GIODO stoi na straży zgodności i legalności przetwarzania danych osobowych w Polsce. W ramach swoich uprawnień, GIODO ma możliwość prowadzenia kontroli u wszystkich podmiotów przetwarzających dane osobowe, czyli zarówno u administratorów danych jak też u podmiotów, które przetwarzają dane wyłącznie na zlecenie administratora danych. GIODO posiada uprawnienia do przeprowadzenia kontroli również w kancelarii prawnej. Kontrola dotycząca przetwarzania danych w kancelarii prawnej może zostać ograniczona wyłącznie do danych, które nie będą stanowić tajemnicy zawodowej radcy prawnego. Jeśli jednakże w toku czynności kontrolnych inspektorzy GIODO stwierdzą, że informacje, objęte ochroną wynikającą z art. 3 urp nie są chronione w sposób zapewniający im poufność, należy liczyć się z możliwością powiadomienia o takiej sytuacji dziekana okręgowej izby, na terenie której stwierdzono naruszenie, co może wiązać się z wszczęciem postepowania dyscyplinarnego wobec odpowiedzialnego radcy prawnego.

10. Jakie zabezpieczenia powinny zostać wprowadzone w kancelarii?

Do zabezpieczenia przetwarzania danych w kancelarii należy podejść kompleksowo, biorąc pod uwagę wszystkie czynniki wpływające na bezpieczeństwo danych. Wdrożenie pojedynczych środków ochrony może być nieskuteczne, a co gorsze, może utwierdzać w błędnym przekonaniu zapewnienia bezpieczeństwa. Z drugiej strony, zastosowanie zbyt wielu środków ochrony może znacznie utrudnić świadczenie usług, a niedostosowanie środków do zaistniałych okoliczności prowadzić do wykształcenia się „dróg na skróty" oraz „rozwiązań tymczasowych" wśród pracowników, co w efekcie może doprowadzić do spadku poziomu bezpieczeństwa. Przy projektowaniu środków bezpieczeństwa danych osobowych dobrze jest wspierać się rozwiązaniami opracowanymi przez organizacje zajmujące się normami

zarządzania, np. ISO/IEC 27001 Zarządzanie bezpieczeństwem informacji. Niezależnie od wykorzystanych standardów przy projektowaniu systemu bezpieczeństwa należy brać pod uwagę bezpieczeństwo fizyczne (fizyczny dostęp do danych i dokumentów, zabezpieczenie lokalu, pomieszczeń w których przetwarzane są dane osobowe), organizacyjne (odpowiedzialność osób, realizacja praw osób, których dane dotyczą), prawne (legalność przetwarzania, klauzule umowne) oraz technologiczne (systemy informatyczne, urządzenia, nadzór nad systemem, logiczny dostęp do danych).

11. Jak zabezpieczyć przetwarzanie danych zawartych w dokumentach papierowych?

Administrator danych jest odpowiedzialny za dobranie środków ochrony danych adekwatnych do zagrożeń i okoliczności ich przetwarzania. Przetwarzanie danych zawartych w dokumentach papierowych powinno opierać się na kilku podstawowych zasadach:

1) Dostęp do danych powinny posiadać wyłącznie osoby do tego uprawnione/upoważnione.
2) Osoby upoważnione powinny posiadać dostęp wyłącznie do tych danych, które są niezbędne do realizacji ich obowiązków służbowych/zawodowych.
3) Po zakończeniu pracy dokumenty podlegające ochronie należy przechowywać w zamkniętych na klucz szafach i szufladach.
4) Dokumenty zawierające dane osobowe należy niszczyć w sposób zapewniający nieodwracalność tego procesu.
5) Administrator danych powinien mieć kontrolę nad całym procesem przetwarzania dokumentów.

12. Jak zabezpieczyć dane i dokumenty elektroniczne w sieci kancelaryjnej?

Projektując kancelaryjną sieć komputerową należy wziąć pod uwagę funkcje, jakie ma ona spełniać. Szczególnej uwagi wymaga stosowanie rozwiązań technicznych umożliwiające dostęp do danych kancelarii poprzez połączenie z zewnątrz kancelarii – z Internetu. Takie rozwiązanie powinno być odpowiednio przygotowane i zabezpieczone, bowiem wykorzystanie tego kanału przez osoby nieuprawnione może narazić wszystkie dane na utratę poufności. Dostęp do sieci kancelaryjnej powinien odbywać się wyłącznie po prawidłowym uwierzytelnieniu użytkownika, za pomocą indywidualnie nadanego identyfikatora (loginu) oraz okresowo zmienianego hasła o odpowiedniej sile, a udzielanie takiego dostępu powinno być monitorowane i przechowywane w logach systemowych. Uprawnienia do zasobów wspólnych w sieci kancelaryjnej należy nadawać wyłącznie osobom, którym jest to niezbędne. Pewna część zasobów, jak też uprawnienia administracyjne do urządzeń sieci powinna być przydzielana wyłącznie wybranym osobom. Dostęp do danych powinien być monitorowany, a system powinien umożliwiać weryfikację dokonanych przez poszczególnych użytkowników operacji na danych.

13. Jak zabezpieczyć się przed zagrożeniami z Internetu oraz oprogramowaniem złośliwym?

Obecnie dostęp do sieci Internet jest wszechobecny. Jednocześnie, to właśnie Internet może być poważnym źródłem zagrożeń dla danych przetwarzanych w sieci kancelaryjnej. Ruch pomiędzy siecią kancelaryjną a Internetem powinien być monitorowany a logi przechowywane. Nadzór nad dostępem do Internetu powinno zapewniać specjalne oprogramowanie lub urządzenie Firewall. Dostęp do sieci Internet powinien być również kontrolowany za pomocą serwera (lub oprogramowania) pośredniczącego – Proxy. Udostępnianie połączenia internetowego dla urządzeń innych, niż należące do kancelarii (urządzenia mobilne pracowników, dostęp do sieci dla klientów) powinno odbywać się w ramach wydzielonej specjalnej podsieci, odseparowanej od sieci kancelaryjnej, która zapewniałaby klientom kancelarii bezprzewodowy dostęp do Internetu. W tym przypadku należy upewnić się, że taka sieć jest w pełni odseparowana od sieci kancelaryjnej. Użytkownicy w sieci kancelaryjnej nie powinni posiadać pełni uprawnień administracyjnych. W szczególności konta użytkowników komputerów osobistych powinny mieć ograniczone uprawnienia. Oprogramowanie złośliwe może wykorzystywać uprawnienia użytkowników w celu uzyskania dostępu

do funkcji niedostępnych dla zwykłych użytkowników. Na stacjach roboczych powinno być zainstalowane oprogramowanie antywirusowe. Oprogramowanie powinno być stale aktywne oraz aktualizowane na bieżąco ze strony dostawcy. Wszelkie urządzenia oraz dyski przenośne, podłączane do sieci kancelaryjnej (np. do jednego z komputerów w sieci) powinny być skanowane w celu wykrycia złośliwego oprogramowania przed pierwszym uruchomieniem i za każdym razem, gdy były wykorzystywane w obcej sieci (np. po powrocie od klienta).

14. Jak zabezpieczyć dane na urządzeniach przenośnych?

Przetwarzanie danych w formie elektronicznej obecnie coraz częściej odbywa się za pomocą przenośnych urządzeń. Mogą to być zarówno laptopy, jak też tablety czy smartfony. Dane mogą być również przechowywane na przenośnych dyskach pamięci. W przypadku urządzeń przenośnych ryzyko związane z dostępem osób nieupoważnionych do danych przechowywanych na tych nośnikach jest istotnie zwiększone, dlatego powinny one być objęte ścisłym nadzorem. Niezależnie od tego, o jakim typie urządzenia jest mowa, absolutnym minimum jest szyfrowanie zawartości takiego urządzenia. Dzięki wprowadzeniu szyfrowania zapobiegamy dostępowi osób nieupoważnionych do danych zawartych na nośniku pomimo jego utraty. Równie ważna jest odpowiedź na pytanie, czy dostęp pracowników kancelarii do danych chronionych z wykorzystaniem smartfonów jest konieczny dla sprawnego wykonywania ich obowiązków. Jeśli chcemy, aby pracownicy posiadali dostęp do danych w każdym momencie, należy rozważyć wprowadzenie szyfrowania danych urządzenia, blokowanie urządzenia hasłem podczas nieobecności. Jeśli jednak wdrożenie środków ochrony okaże się zbyt kosztowne dla organizacji – należy zminimalizować możliwość przechowywania danych da urządzeniach przenośnych. Warto również stosować środki umożliwiające zdalne zarządzanie urządzeniami przenośnymi, w tym opcję zdalnego usunięcia danych z nośnika.

15. Jak zabezpieczyć dane przesyłane emailem?

Często spotykamy się z koniecznością przekazania danych za pomocą wiadomości elektronicznych. Przy zabezpieczeniu poczty elektronicznej należy brać pod uwagę zarówno bezpieczeństwo danych przesyłanych w sieci, jak też bezpieczeństwo danych przechowywanych na serwerach pocztowych. Przy korzystaniu z poczty elektronicznej należy pamiętać o kilku zasadach:

1) Należy starannie dobierać dostawcę serwera poczty elektronicznej. Dostawcy darmowych rozwiązań zazwyczaj nie zapewniają poufności danych przechowywanych na serwerach pocztowych. Przy wyborze dostawcy zawsze należy zwracać uwagę na gwarantowane zasady poufności oraz jego zakres odpowiedzialności.
2) Wiadomości pomiędzy serwerami zwykle przesyłane są w sposób jawny, który nie zapewnia poufności danych. W celu zabezpieczenia poufności danych wiadomości przesyłane mailem powinny być zaszyfrowane. Istnieje wiele możliwości szyfrowania wiadomości. Jeśli nie mamy pewności, co do bezpieczeństwa, należy co najmniej zaszyfrować samą treść (np. plik załączony do wiadomości), a hasło do odszyfrowania przesłać innym kanałem komunikacji (np. sms).
3) Należy poinformować klienta oraz ustalić z nim sposób wymiany informacji, zanim zostanie on wykorzystany. W przypadku wyboru elektronicznej wymiany informacji, klient powinien zostać uprzedzony o zagrożeniach takiego rozwiązania. Można też zawczasu ustalić z klientem, jakie środki będą wykorzystywane do zabezpieczenia wymiany danych w tym kanale komunikacji.

16. Jak właściwie niszczyć dane?

Właściwe niszczenie danych jest jednym z kluczowych wymagań, jakie należy wdrożyć w kancelarii. Niezależnie od wybranego sposobu niszczenia należy pamiętać o tym, że niszczenia danych jest skuteczne wyłącznie wtedy, gdy niemożliwe jest odtworzenie informacji podlegającej zniszczeniu. Należy przy tym pamiętać, że wyrzucenie do kosza lub przeniesienie do kosza w systemie nie zapewnia skuteczności niszczenia dokumentu. Do niszczenia należy

wykorzystywać przeznaczone ku temu narzędzia. Do niszczenia dokumentów papierowych można stosować niszczarki dokumentów. Należy przy tym wziąć pod uwagę, że istnieje kilka rodzajów niszczarek. Niszczarki oznaczane są obecnie według normy DIN 66399. Wymóg ochrony danych dzieli się na 3 klasy. Typ danych jest kontrolowany w celu określenia wymagania sposobu ich ochrony, co wskazuje, jakie wymagania są potrzebne do ochrony danych związane z klasą ochrony. Do niszczenia dokumentów zawierających dane osobowe należy stosować niszczarki klasy 2 lub 3. Do niszczenia dokumentów w formie papierowej można również skorzystać z usług firm utylizacyjnych. W tym przypadku zabezpieczony pojemnik na dokumenty dostarczany jest do wybranej lokalizacji. W pojemniku umieszcza się dokumenty przeznaczone do utylizacji. We wspólnie określonym terminie firma utylizująca organizuje proces spalenia dokumentów lub utylizacji z wykorzystaniem innych środków. Dla skutecznego niszczenia danych elektronicznych zalecane jest wykorzystanie specjalnie przeznaczonego w tym celu narzędzia – oprogramowania, które wielokrotnie nadpisuje dane zawarte na dysku w miejscu, gdzie zapisany był dokument. Usunięcie pliku za pomocą funkcji podstawowych zawartych w systemie informatycznym nie powoduje fizycznego usunięcia danych, a jedynie wymazanie adresu, pod jakim jest on zapisany na dysku. Za pomocą prostego oprogramowania istnieje możliwość odtworzenia takich dokumentów. Szczególną uwagę należy zwrócić na bardzo popularne nośniki USB (pendrive). W przypadku konieczności zniszczenia całego dysku, należy zastosować inne metody utylizacji – np. zanurzenie w kwasie lub demagnetyzacja – które niszczą bezpowrotnie cały nośnik danych.

17. Na co zwrócić uwagę przy wykorzystywaniu usług internetowych?

Przy realizacji działań zawodowych coraz częściej wykorzystywane są usługi firm zewnętrznych. Rozwiązania dostępne na rynku oparte są w większości na tzw. rozwiązaniach chmurowych. Tym terminem obecnie określa się wszelkie usługi, korzystające z rozwiązań opartych o przetwarzanie danych w środowisku internetowym (np. wystawianie faktur, organizacja pracy, systemy informacji prawnej, kalendarze, itp.). Wykorzystanie usług chmurowych łączy się z ryzykiem powierzenia danych innemu podmiotowi, który może nie zapewniać właściwego poziomu bezpieczeństwa, w tym samemu posiadać nieograniczony dostęp do powierzonych danych zatem wybór dostawcy rozwiązania powinien zostać dokonany ze szczególną uwagą. Pomocnym przy wyborze dostawcy oraz projektowaniu środków bezpieczeństwa może być dokument przygotowany przez GIODO dla organów administracji publicznej, znajdujący się pod adresem: http://www.giodo.gov.pl/259/id_art/6271/j/pl.

18. Relacje z podmiotami trzecimi przetwarzającymi dane w imieniu i na rzecz kancelarii (firmy księgowe, doradztwa personalnego, obsługi informatycznej)

Przy projektowaniu zabezpieczeń danych przetwarzanych w kancelarii nie możemy zapominać o tym, że część usług może być dostarczana przez dostawców zewnętrznych. W przypadku, gdy usługa polegać będzie (choćby pośrednio) na przetwarzaniu danych osobowych i takie przetwarzanie odbywać się będzie z wykorzystaniem narzędzi dostawcy – należy sporządzić stosowną umowę powierzenia, w której należy określić zakres i cel przetwarzania danych przez dostawcę, jak również warunki oraz zasady bezpieczeństwa, które obowiązany jest wdrożyć i stosować dostawca. Dobrą praktyką jest również zapewnienie prawa do kontroli wykonania umowy, w tym zabezpieczenia danych powierzonych takiemu dostawcy oraz zasady ewentualnej możliwości dalszego powierzenia przetwarzania naszych danych przez dostawcę innym podmiotom.

Autor: Marcin Wielisiej – Administrator Bezpieczeństwa Informacji, Data Processing Architects Sp. z o.o.
Współautor: radca prawny Tomasz Wypych – Okręgowa Izba Radców Prawnych w Warszawie
Współpraca merytoryczna: radca prawny Michał Wołoszański – Wołoszański i Wspólnicy Kancelaria Prawna sp.k.