

Warszawa, dn. 4 sierpnia 2026 r.

Jak podpisywać umowy online?

Coraz częściej umowy podpisujemy przez Internet. Jest to zdecydowanie łatwiejsza i przede wszystkim szybsza opcja, dzięki której nie musimy umawiać się na spotkania, drukować dokumentów, jeździć do biura czy czekać na kuriera z papierowymi wersjami umów. Wystarczy kilka kliknięć i sprawa załatwiona po obu stronach umowy.

Jest jednak coś, o czym w pośpiechu łatwo zapomnieć: razem z umową online przesyłamy dane osobowe takie jak imię, nazwisko, adres, numer telefonu, PESEL czy numer konta. A dane te trzeba chronić nie mniej starannie niż wtedy, gdy leżą w segregatorze w szafie. Różnica polega na tym, że w internecie zagrożenia trudniej zauważyć: nie zobaczymy przecież „wycieku” gotym okiem tak, jak zauważylibyśmy zagubioną teczkę z dokumentami.

Żeby pokazać, że to nie jest teoretyzowanie, warto przywołać niedawną jeszcze nieprawomocną decyzję Prezesa Urzędu Ochrony Danych Osobowych (Decyzja DKN.5131.7.2022. z 13 kwietnia 2026 r.) Sprawa dotyczyła firmy sprzedającej energię elektryczną w modelu D2D (door-to-door, czyli sprzedaży bezpośredniej „od drzwi do drzwi”). Handlowcy odwiedzali klientów w domach, podpisywali z nimi papierowe umowy, a później dla wygody zaczęli przysyłać sobie zdjęcia i skany tych dokumentów przez zwykły komunikator internetowy: nieautoryzowany przez firmę i zainstalowany na prywatnych telefonach.

W efekcie jeden z byłych pracowników, który już dawno stracił prawo dostępu do tych danych, nadal miał je na swoim telefonie i pokazał je dziennikarzowi radiowemu jako dowód nieprawidłowości w firmie. Naruszenie dotyczyło danych co najmniej kilkunastu osób, a prawdopodobnie znacznie większej liczby: imion, nazwisk, adresów, numerów PESEL, e-maili i telefonów. Urząd Ochrony Danych Osobowych ukarał grzywną podwykonawcę odpowiedzialnego za tę praktykę (10 145 zł), a spółce oraz pozostałym pośrednikom w tańcu sprzedaży udzielił upomnień każdemu z nich zarzucając, że nie przeanalizował ryzyka związanego z takim sposobem przysyłania danych i nie wdrożył zabezpieczeń adekwatnych do tego ryzyka.

Ta historia to dobry punkt wyjścia do rozmowy o tym, jak bezpiecznie podpisywać umowy przez internet i czego należy pilnować, gdy dokumenty z danymi osobowymi wędrują między różnymi osobami czy systemami.

O czym pamiętać jako podpisujący?

Jeśli to Ty jesteś stroną, która ma podpisać przestaną umowę jako klient, czy jako pracownik podpisujący dokumenty w imieniu firmy: masz prawo być czujny. Oto na co zwrócić uwagę:

1. **Sprawdź, skąd pochodzi wiadomość.** Zanim otworzysz link czy załącznik, upewnij się, że nadawca to rzeczywiście firma, z którą masz do czynienia, a nie ktoś podszywający się pod nią (tzw. phishing, czyli wyłudzenie danych przez fałszywe wiadomości). Podejrzany adres e-mail, literówki w domenie czy nietypowa prośba o „pilne” działanie to sygnały ostrzegawcze.
2. **Korzystaj tylko z kanałów wskazanych przez firmę.** Jeżeli umowa ma zostać podpisana przez dedykowany system do e-podpisów, nie przysyłaj jej dla wygody w prywatnym

komunikatorze czy na prywatną skrzynkę mailową. To właśnie przez nieautoryzowane narzędzie, doszło do naruszenia opisanego w decyzji UODO. Komunikatory konsumenckie bywają szyfrowane, ale zwykle automatycznie zapisują załączniki w pamięci telefonu, a historia rozmów może pozostać nawet po usunięciu osoby z grupy.

3. **Zwróć uwagę, jakie dane przekazujesz.** Do podpisania umowy rzadko potrzebny jest komplet Twoich danych. Jeśli formularz prosi o więcej informacji niż wynika to z charakteru umowy (np. *pełny numer karty płatniczej przy zwykłej umowie abonamentowej*), to moment, by zapytać, dlaczego są one potrzebne. Zasada minimalizacji danych, a więc zbierania tylko tego, co naprawdę niezbędne do realizacji celu przetwarzania to jedna z podstawowych zasad RODO.
4. **Sprawdź zabezpieczenia strony i platformy.** Adres strony powinien zaczynać się od „https”, a nie samego „http” ta dodatkowa litera oznacza, że połączenie jest szyfrowane (czyli dane przesyłane między Twoim urządzeniem a serwerem są zakodowane i trudniejsze do przechwycenia). Warto też zwrócić uwagę, czy platforma do podpisu elektronicznego jest znanym, legalnie działającym dostawcą, a nie przypadkowym narzędziem, o którym nigdy wcześniej nie słyszałeś.
5. **Nie zostawiaj kopii dokumentów w przypadkowych miejscach.** O pobranym PDF z podpisaną umową łatwo zapomnieć w „Pobrane” na telefonie czy w skrzynce mailowej. Jeśli nie musisz go tam trzymać usuń albo przenieś do bezpiecznego, zaszyfrowanego miejsca.
6. **Wiedz, jakie masz prawa.** Jako osoba, której dane dotyczą, masz prawo zapytać administratora (czyli podmiot decydujący o celach i sposobach przetwarzania Twoich danych; w tym przypadku zwykle firmę, z którą zawierasz umowę), jak długo dane będą przechowywane, kto ma do nich dostęp i w jaki sposób są zabezpieczone.

O czym pamiętać jako wysyłający?

Jeśli to Twoja firma wysyła umowy do podpisu klientom, kontrahentom czy pracownikom odpowiedzialność jest jeszcze większa. To właśnie na administratorze danych (*podmiocie decydującym, po co i jak przetwarzane są dane*) oraz na podmiotach przetwarzających (*firmach czy osobach, którym powierzono przetwarzanie danych w naszym imieniu, np. dostawcach systemów*) ciąży obowiązek zapewnienia odpowiedniego bezpieczeństwa danych.

1. **Korzystaj wyłącznie z zatwierdzonych narzędzi.** To najważniejsza lekcja z wyżej wskazanej decyzji UODO. Żaden pracownik, agent czy podwykonawca nie powinien na własną rękę wprowadzać dodatkowych aplikacji czy komunikatorów do przesyłania dokumentów z danymi klientów, nawet jeśli robi to dla usprawnienia pracy. W sprawie energetycznej spółki nikt formalnie nie zaakceptował komunikatora, którego używano do wymiany skanów umów, a mimo to ta praktyka trwała miesiącami, zanim wyszła na jaw.
2. **Zadbaj o umowy powierzenia z podwykonawcami.** Jeśli w proces sprzedaży czy obsługi klienta zaangażowani są zewnętrzni agenci, przedstawiciele handlowi czy inne firmy, konieczne jest zawarcie z nimi umowy powierzenia przetwarzania danych osobowych, zgodnie z art. 28 RODO. Sama umowa to jednak nie wszystko: organ nadzorczy podkreślił, że

kluczowe jest też bieżące weryfikowanie, czy te podmioty faktycznie stosują się do ustalonych zasad, a nie tylko podpisanie dokumentu na wszelki wypadek.

3. **Przeprowadź analizę ryzyka i rób to regularnie.** RODO wymaga, by przed rozpoczęciem przetwarzania danych (a potem cyklicznie) ocenić, jakie zagrożenia wiążą się z danym procesem, i dobrać do nich odpowiednie zabezpieczenia. W omawianej sprawie żaden z uczestników łańcucha sprzedaży: ani firma, ani żaden z pośredników nie przewidział, że pracownicy pracujący w terenie, z dala od biura, będą szukać nieformalnych „skrótów” ułatwiających im pracę.
4. **Szkol i przypominaj regularnie.** Samo przeszkolenie pracownika przy zatrudnieniu nie wystarczy. Warto okresowo przypominać zespołowi o zasadach bezpiecznego przetwarzania danych, zwłaszcza jeśli pracują oni poza biurem, z dostępem do danych klientów na urządzeniach mobilnych.
5. **Kontroluj, nie tylko ufaj.** Nadzór nad podwykonawcami to nie jednorazowa weryfikacja przy podpisywaniu umowy, ale stały proces: audyty, kontrole, ankiety, rozmowy. UODO wprost wskazał, że administrator ma obowiązek weryfikować, czy podmiot przetwarzający „daje wystarczające gwarancje” bezpieczeństwa i to w sposób ciągły, a nie tylko na starcie współpracy.
6. **Ogranicz to, co przesyłasz.** Jeżeli do podpisania umowy nie jest potrzebny pełny numer PESEL czy skan dowodu osobistego nie umieszczaj tych danych w treści wiadomości czy w niezabezpieczonym pliku. Jeśli już muszą zostać przesłane, korzystaj z systemów, które szyfrują dane w trakcie przesyłania i przechowywania, a nie ze zwykłej poczty e-mail czy komunikatora. Ewentualnie, jeśli wysłanie dokumentów mailem jest jedyną opcją: zahasłuj plik (może być to nawet zwykły zip7) i hasło przekaz podpisującemu za pomocą innego kanału komunikacji np. SMS-em.
7. **Miej plan na wypadek naruszenia.** Nawet przy najlepszych zabezpieczeniach coś może pójść nie tak. Warto mieć przygotowaną procedurę zgłaszania naruszeń zarówno wewnątrz firmy, jak i do UODO (na zgłoszenie jest 72 godziny od stwierdzenia naruszenia). W opisanej sprawie firma, która zgłosiła naruszenie z własnej inicjatywy, została potraktowana łagodniej niż podwykonawca, który próbował umniejszać swoją rolę i był niekonsekwentny w wyjaśnieniach.

Słowo o podpisie elektronicznym

Przy okazji tematu podpisywania umów warto wspomnieć o samym podpisie elektronicznym, bo to on często budzi największe wątpliwości.

W Polsce funkcjonują różne jego rodzaje: **podpis zaufany** (bezpłatny, powiązany z profilem zaufanym, używany m.in. w kontaktach z urzędami), **podpis kwalifikowany** (płatny, o najwyższej mocy prawnej, równoważny podpisowi odręcznemu) oraz różne **podpisy elektroniczne** oferowane przez komercyjne platformy do obiegu dokumentów. Wybór odpowiedniego rodzaju podpisu zależy od charakteru umowy i wymogów prawnych, jakie musi ona spełniać, ale niezależnie od tego, jakiego

podpisu używamy, samo bezpieczne przesłanie dokumentu do podpisania jest równie istotne, co sam moment złożenia podpisu.

Checklista przed wysłaniem dokumentów

Zanim klikniesz „wyślij”, warto przejść przez taką krótką listę kontrolną:

- Czy dokument wysyłany jest przez zatwierdzony, oficjalny kanał (system do podpisów, firmowa poczta), a nie prywatny komunikator lub prywatny e-mail?
- Czy w treści dokumentu i wiadomości znajdują się tylko te dane, które są rzeczywiście niezbędne do zawarcia umowy?
- Czy połączenie i platforma, z której korzystasz, są zabezpieczone (szyfrowanie, weryfikacja tożsamości nadawcy i odbiorcy)?
- Czy odbiorca dokumentu jest właściwą, zweryfikowaną osobą (upewnij się co do adresu e-mail czy numeru telefonu)?
- Czy masz wdrożoną umowę powierzenia przetwarzania danych, jeśli w procesie uczestniczy podmiot zewnętrzny (np. agent, platforma do e-podpisów)?
- Czy dostęp do systemu wysyłki mają wyłącznie upoważnione osoby, z indywidualnymi loginami i silnymi hasłami?
- Czy wiesz, jak długo dokument (i dane w nim zawarte) będzie przechowywany i kto go usunie, gdy nie będzie już potrzebny?
- Czy masz procedurę na wypadek, gdyby dokument trafił do niewłaściwej osoby albo doszło do innego naruszenia?

Podsumowanie

Wygoda podpisywania umów przez internet nie musi kolidować z bezpieczeństwem danych pod warunkiem, że obie strony, czyli podpisujący i wysyłający, zachowują czujność. Historia decyzji UODO pokazuje, że nawet duże firmy mogą stracić kontrolę nad danymi swoich klientów, jeśli zaufają nieformalnym usprawnieniom wprowadzanym w terenie, bez odpowiedniej analizy ryzyka i kontroli. Dobra wiadomość jest taka, że wystarczy kilka prostych nawyków: korzystanie z zatwierdzonych narzędzi, ograniczanie zakresu przesyłanych danych i regularna weryfikacja tego, co dzieje się „w praktyce”, żeby znacząco zmniejszyć ryzyko podobnych problemów.

Gabriela Tokarska - młodsza specjalistka ds. ochrony danych osobowych w iSecure sp. z o.o.