Cyberbezpieczeństwo w księgowości – obowiązki i ryzyka prawne

Ani Sokołowska - Prawnik w JCJK Kancelaria Prawna w Krakowie, Prezes Zarządu Cluster Solutions sp. z o.o.

enova 365

JCJK
KANCELARIA PRAWNA

Dlaczego księgowość to cel numer jeden dla cyberataków?

Wartość danych

Księgowi przetwarzają najbardziej wrażliwe informacje:

- Dane finansowe przedsiębiorstw
- Informacje osobowe pracowników
- Poufne strategie biznesowe
- Dokumenty podatkowe i sprawozdawcze

Konsekwencje incydentów

Każde naruszenie bezpieczeństwa niesie ze sobą:

- Odpowiedzialność prawną i finansową
- Utratę zaufania klientów
- Szkody reputacyjne
- Potencjalne sankcje regulatorów

Fundament prawny: kluczowe regulacje - cyberbezpieczeństwo

1

#**RODO**

2

#**Ustawa o świadczeniu usług drogą elektroniczną**

#**Prawo komunikacji elektronicznej**

3

#**Ustawa o Krajowym systemie cyberbezpieczeństwa**

#**NIS, NIS2**

4

Inne np.:

#Ustawa o rachunkowości

#Ordynacja podatkowa,

#Ustawa o CIT/PIT,

#Rozporządzenia JPK i KPiR,

#KSeF (ustawa o VAT),

#Miedzyn.Stand.Sprawozd.Finan.

Obowiązki i ryzyka prawne: PKE i NIS2

Prawo komunikacji elektronicznej (PKE)

Obowiązki prawne:

- Zapewnienie tajemnicy komunikacji (szyfrowanie, certyfikaty SSL) i ochrona danych przed nieuprawnionym dostępem.
- Ograniczenie przetwarzania danych do niezbędnego minimum.

Ryzyka prawne:

- Kary administracyjne od UKE za naruszenie tajemnicy komunikacji.
- Roszczenia cywilne klientów za ujawnienie danych.

NIS2 / Krajowy System Cyberbezpieczeństwa (KSC)

Obowiązki prawne:

- Wdrożenie technicznych zabezpieczeń (MFA, backupy, segmentacja sieci).
- Prowadzenie procedur reagowania i zgłaszanie poważnych incydentów do organów nadzorczych (np. CSIRT).

Ryzyka prawne:

- Wysokie kary administracyjne (do 10 mln € / 2% obrotu).
- Odpowiedzialność cywilna i osobista kierownictwa za brak zabezpieczeń.

Pośredni wpływ ustawy krajowej o cyberbezpieczeństwie i NIS2 na Księgowych

Obsługa klientów objętych ustawą

Klienci objęci ustawą (np. duże firmy) wymagają od biur rachunkowych (jako współpracowników) wdrożenia standardów cyberbezpieczeństwa (np. szyfrowanie, kopie zapasowe).

Łańcuch dostaw

Biura rachunkowe jako część łańcucha dostaw dużych przedsiębiorstw są audytowane i muszą udowadniać zgodność z wymogami bezpieczeństwa podyktowanymi ustawą.

Przyszła nowelizacja NIS2/UKSC 2025

Duże biura rachunkowe mogą zostać uznane za *"ważne podmioty"* w przyszłej nowelizacji UKSC (2025). Oznacza to bezpośrednie obowiązki (SZBI, zgłaszanie incydentów) i ryzyko kar.

Obowiązki i ryzyka prawne: UŚUDE i KSeF

UŚUDE i KSeF wprowadzają specyficzne wymogi cyberbezpieczeństwa dla biur rachunkowych, generując kluczowe obowiązki i potencjalne ryzyka prawne.

Ustawa o świadczeniu usług drogą elektroniczną (UŚUDE)

Obowiązki prawne:

- Zapewnienie bezpieczeństwa systemów IT.
- Ochrona danych elektronicznych przed wyciekiem.

Ryzyka prawne:

- Kary administracyjne (UOKiK).
- Odpowiedzialność cywilna za wyciek danych.
- Utrata reputacji i odpowiedzialność kontraktowa.

KSeF (Krajowy System e-Faktur)

Obowiązki prawne:

- Bezpieczna autoryzacja (certyfikaty, tokeny).
- Kontrola dostępu do systemu KSeF.
- Bezpieczeństwo archiwizacji faktur.

Ryzyka prawne:

- Sankcje podatkowe za błędy dostępu.
- Odpowiedzialność karno-skarbowa.
- Ryzyko odpowiedzialności wobec klienta za utratę faktur.

Obowiązki i ryzyka prawne: JPK i RODO

Jednolity Plik Kontrolny (JPK)

Obowiązki prawne:

- Bezpieczne przesyłanie danych (szyfrowanie transmisji).
- Stosowanie certyfikowanego oprogramowania do generowania JPK.
- Archiwizacja plików JPK z zabezpieczeniem przed modyfikacją.

Ryzyka prawne:

- Sankcje karno-skarbowe za błędy w danych JPK.
- Odpowiedzialność za naruszenie bezpieczeństwa przesyłanych danych.
- Roszczenia klientów z powodu błędów biura.

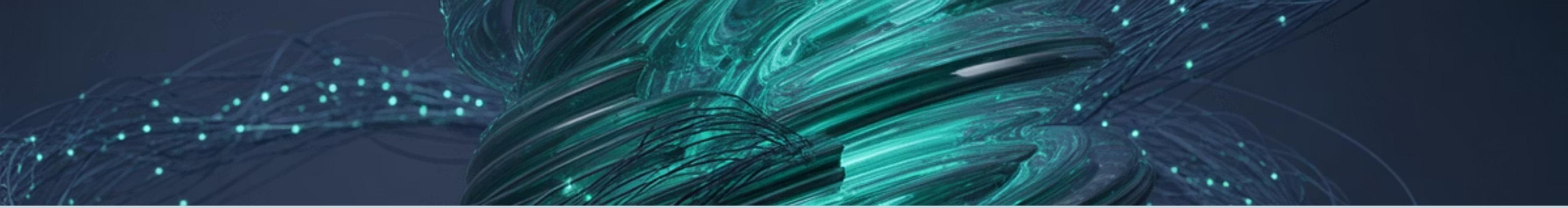
RODO (Ogólne Rozporządzenie o Ochronie Danych)

Obowiązki prawne:

- Ochrona danych osobowych (szyfrowanie, MFA, backupy).
- Wdrożenie odpowiednich procedur i zabezpieczeń tech./org. (art. 32 RODO).
- Zawieranie umów powierzenia przetwarzania danych z klientami + weryfikacja drugiej strony.
- Zgłaszanie naruszeń do UODO (72h) i informowanie klientów.
- Wybór dostawców chmurowych zapewniających zgodność z RODO.

Ryzyka prawne:

- Kary finansowe: do 20 mln € lub 4% rocznego obrotu.
- Roszczenia odszkodowawcze od klientów.
- Odpowiedzialność osobista osób zarządzających.



Najczęstsze zagrożenia w praktyce księgowej - część 1

Poniżej przedstawiamy kluczowe zagrożenia cyberbezpieczeństwa, z którymi biura rachunkowe i księgowi spotykają się na co dzień:

Phishing i spoofing

Fałszywe maile i SMS-y podszywające się pod KSeF, banki czy Ministerstwo Finansów. Kliknięcie w złośliwy link może prowadzić do kradzieży danych logowania lub infekcji komputera.

Ataki ransomware

To rodzaj ataku hakerskiego, w którym **przestępcy blokują dostęp do Twoich danych** – najczęściej je szyfrują. Pliki (księgi rachunkowe, faktury, listy płac, JPK) nagle stają się **nieczytelne** i nie można ich otworzyć.

Nieuprawniony dostęp

Zbyt szerokie uprawnienia dostępu lub brak uwierzytelniania dwuskładnikowego (MFA) to prosta droga do kradzieży lub modyfikacji wrażliwych danych finansowych.

Wycieki danych

Księgowi przetwarzają listy płac, numery PESEL i rachunki bankowe. Utrata niezaszyfrowanego laptopa czy pendrive'a to poważne naruszenie RODO.

Brak lub błędne backupy

Kopie zapasowe przechowywane tylko lokalnie są bezużyteczne po ataku ransomware. Brak bezpiecznych kopii offline lub w chmurze to ryzyko utraty danych.

KSeF i nowe systemy MF

Integracja wymaga bezpiecznych API i certyfikatów. Błędy konfiguracyjne mogą otworzyć cyberprzestępcom drogę do przejęcia komunikacji z urzędem.

Najczęstsze zagrożenia w praktyce księgowej - część 2

Fałszywe aktualizacje

Cyberprzestępcy podszywają się pod dostawców oprogramowania księgowego. Instalacja takiej "aktualizacji" może skutkować przejęciem kontroli nad całym systemem.

Niezgodna chmura

Korzystanie z darmowych lub niesprawdzonych usług chmurowych, zwłaszcza tych z centrami danych poza UE -**RODO dopuszcza chmurę w państwach trzecich**, ale tylko wtedy, gdy:

- państwo to ma decyzję Komisji Europejskiej o **odpowiednim poziomie ochrony**, albo
- dostawca stosuje **Standardowe Klauzule Umowne (SCC)**

Ataki socjotechniczne (telefon)

Oszuści podszywają się pod "urzędników", "bankowców" lub klientów, wywierając presję na księgowych w celu wyłudzenia poufnych informacji.

Prywatne urządzenia

Logowanie do systemów firmowych z niezabezpieczonego prywatnego laptopa lub telefonu tworzy lukę bezpieczeństwa, mogącą prowadzić do wycieku danych.

Złośliwe dodatki i keyloggery

Darmowe wtyczki do przeglądarek mogą rejestrować loginy i hasła, dając przestępcom dostęp do bankowości online lub KSeF.

Błędy ludzkie

Wysłanie faktury na błędny adres e-mail lub wpisanie niewłaściwego NIP-u to naruszenie danych osobowych, wymagające zgłoszenia do UODO w ciągu 72 godzin.

Odpowiedzialność Księgowych

Cywilna / zawodowa

Odpowiedzialność za szkody klienta lub pracodawcy (np. wyciek danych finansowych).

Administracyjna

Sankcje dla firmy za brak procedur cyberbezpieczeństwa, konsekwencje dla osób obsługujących dane.

Karno–prawna

Naruszenia ochrony danych osobowych (np. nieuprawnione ujawnienie, brak zgłoszenia incydentu).

Etyczna / reputacyjna

Utrata zaufania klientów i odpowiedzialność zawodowa wobec organizacji branżowych.

Praktyczny katalog obowiązków księgowego

Minimalizacja danych

Przetwarzaj tylko te dane, które są niezbędne do realizacji usług księgowych.

Bezpieczna komunikacja

Korzystaj wyłącznie z szyfrowanych kanałów komunikacji i sprawdzonych rozwiązań chmurowych z certyfikatami bezpieczeństwa.

Zabezpieczenia w umowach

Wprowadzaj do kontraktów z klientami i dostawcami IT szczegółowe klauzule dotyczące cyberbezpieczeństwa, podziału odpowiedzialności !!!

Procedury incydentowe

Przygotuj i wdróż szczegółowe procedury reagowania na incydenty zgodne z wymogami RODO i przyszłej ustawy UKSC. Testy penetracyjne! Nowe wytyczne PUODO!

Szkolenia pracowników

Organizuj systematyczne szkolenia z cyberhigieny, rozpoznawania zagrożeń i właściwego reagowania na podejrzane sytuacje.

Kopie zapasowe

Twórz i regularnie testuj szyfrowane kopie zapasowe, przechowywane w sposób bezpieczny, preferowane offline.

Dziękuję za uwagę!

enova365

JCJK
KANCELARIA PRAWNA