Warszawa, dnia 29 czerwca 2016 r.

Poz. 932

# ROZPORZĄDZENIE
# MINISTRA FINANSÓW[1)]

z dnia 24 czerwca 2016 r.

**w sprawie sposobu przesyłania za pomocą środków komunikacji elektronicznej ksiąg podatkowych oraz wymagań technicznych dla informatycznych nośników danych, na których te księgi mogą być zapisane i przekazywane**

Na podstawie art. 193a § 3 ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2015 r. poz. 613, z późn. zm.[2)]) zarządza się, co następuje:

**§ 1.** Rozporządzenie określa:

1) sposób przesyłania za pomocą środków komunikacji elektronicznej ksiąg podatkowych, części tych ksiąg oraz dowodów księgowych w postaci elektronicznej, zwanych dalej „księgami”;

2) wymagania techniczne dla informatycznych nośników danych, na których księgi mogą być zapisane i przekazywane.

**§ 2.** 1. Księgi mogą być przesyłane za pomocą oprogramowania interfejsowego dostępnego na stronie, której adres jest podany w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych.

2. Księgi przesyłane w sposób, o którym mowa w ust. 1, są opatrzone kwalifikowanym podpisem elektronicznym w rozumieniu art. 3 pkt 12 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73).

3. Sposób opatrywania ksiąg kwalifikowanym podpisem elektronicznym, o którym mowa w ust. 2, określa załącznik do rozporządzenia.

4. Struktura logiczna urzędowego poświadczenia odbioru ksiąg jest udostępniona w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych.

5. Urzędowe poświadczenie odbioru wydane przez elektroniczną skrzynkę podawczą systemu teleinformatycznego administracji podatkowej, po przeprowadzeniu prawidłowej weryfikacji struktury logicznej, poprawności danych i podpisu elektronicznego:

1) zapewnia integralność przekazanych ksiąg zgodnie z przepisami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 oraz z 2016 r. poz. 352);

2) zawiera datę i godzinę przekazania ksiąg i stanowi dowód doręczenia dokumentu.

**§ 3.** 1. Informatyczne nośniki danych, na których księgi mogą być zapisane i przekazywane, są:

1) oznakowane w sposób pozwalający na jednoznaczną identyfikację nośnika;

---

1) Minister Finansów kieruje działem administracji rządowej – finanse publiczne, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Finansów (Dz. U. poz. 1900).

2) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2015 r. poz. 699, 978, 1197, 1269, 1311, 1649, 1923, 1932 i 2184 oraz z 2016 r. poz. 195, 615 i 846.

2) przystosowane do przenoszenia pomiędzy powszechnie dostępnymi urządzeniami odczytującymi;

3) dostosowane do przechowywania w temperaturze 18–22$^{o}$C przy wilgotności względnej 40–50%.

2. Informatyczne nośniki danych, o których mowa w ust. 1, powinny zapewniać możliwość wiernego odczytywania danych w urządzeniach produkowanych przez różnych producentów, właściwych dla danego typu nośnika.

**§ 4.** Rozporządzenie wchodzi w życie z dniem 1 lipca 2016 r.

Minister Finansów: wz. *W. Janczyk*

Załącznik do rozporządzenia Ministra Finansów
z dnia 24 czerwca 2016 r. (poz. 932)

# SPOSÓB OPATRYWANIA KSIĄG KWALIFIKOWANYM PODPISEM ELEKTRONICZNYM WERYFIKOWANYM PRZY POMOCY WAŻNEGO KWALIFIKOWANEGO CERTYFIKATU

Przyjmuje się następujące zasady opatrywania kwalifikowanym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu ksiąg:

1) księgi opatruje się podpisem elektronicznym z wykorzystaniem formatu określonego przez specyfikację techniczną ETSI TS 103 171 XML Advanced Electronic Signatures (XAdES Basic Electronic Signature, w skrócie XAdES-BES) wydaną przez European Telecommunications Standards Institute, w którym do przygotowania formy kanonicznej księgi wykorzystano standardową metodę wyspecyfikowaną w standardzie XMLDSIG oraz treść podpisywanej księgi została umieszczona w elemencie ds:Object;

2) algorytmem kwalifikowanego podpisu elektronicznego jest Sha-1WithRSAEncryption, którego specyfikacja techniczna jest jednoznacznie określona przez następujący identyfikator obiektu: identyfikator iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha1-with-rsa-signature(5);

3) algorytmem kwalifikowanego podpisu elektronicznego jest Sha256WithRSAEncryption, którego specyfikacja techniczna jest jednoznacznie określona przez następujący identyfikator obiektu: identyfikator iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11);

4) algorytmem szyfrowania jest RSA, którego specyfikacja techniczna jest jednoznacznie określona przez następujący identyfikator obiektu: identyfikator joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryptionAlgorithm(1) 1;

5) funkcją skrótu jest SHA-1, którego specyfikacja techniczna jest jednoznacznie określona przez następujący identyfikator obiektu: identyfikator iso(1) identifiedOrganization(3) oIW(14) oIWSecSig(3) oIWSecAlgorithm(2) hashAlgorithmIdentifier(26);

6) funkcją skrótu jest SHA-256, którego specyfikacja techniczna jest jednoznacznie określona przez następujący identyfikator obiektu: identyfikator joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) hashAlgs(2) sha256(1);

7) kwalifikowany certyfikat zawiera w polu identyfikatora podmiotu „subject” przynajmniej następujące atrybuty: nazwa kraju, nazwisko, imię (imiona) lub pseudonim, numer seryjny;

8) wykorzystany zostanie certyfikat kwalifikowany;

9) format, o którym mowa w pkt 1, zawiera w szczególności parametry identyfikujące jednoznacznie certyfikat kwalifikowany podmiotu podpisującego (nazwa wystawcy certyfikatu i jego numer seryjny oraz wartość skrótu SHA-1 lub SHA-256 z certyfikatu), którego używa się podczas weryfikacji podpisu, jest umieszczony w atrybucie podpisanym, którego specyfikacja techniczna jest określona przez następujący znacznik: SigningCertificate oraz treść kwalifikowanego certyfikatu X.509 jest umieszczona w elemencie ds:X509Data, zawartym w elemencie Keylnfo.