**Všeobecná pravidla elektronického podání:**

1. Podle ustanovení § 40 odst. 3 zákona č. 40/1964 Sb., občanský zákoník, je písemný právní úkon platný, je-li podepsán jednající osobou; činí-li právní úkon více osob, nemusí být jejich podpisy na téže listině, ledaže právní předpis stanoví jinak. Pokud je právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky za podmínek stanovených zákonem č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů. V případě, že podání podává orgán veřejné moci, a to z důvodů vylučujících jinak závazné užití informačního systému datových schránek, je povinnen podání opatřit výlučně zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu vydávaným akreditovaným poskytovatelem certifikačních služeb („uznávaný elektronický podpis").

2. Pokud je podání učiněno prostřednictvím informačního systému datových schránek a je učiněno fyzickou osobou, pro niž byla datová schránka zřízena, podnikající fyzickou osobou, pro niž byla datová schránka zřízena, statutárním orgánem právnické osoby, členem statutárního orgánu právnické osoby nebo vedoucím organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku, jednající za právnickou osobu, pro niž byla datová schránka zřízena, nebo jimi pověřenou osobou, má podání stejné účinky jako úkon učiněný písemně a podepsaný, ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob, tedy podpis příslušné osoby je nahrazen autentizací provedenou uvedeným informačním systémem (§ 18 odst. 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů).

3. Pokud by ministerstvu bylo doručeno elektronické podání, které by nebylo opatřeno elektronickým podpisem podle výše uvedených pravidel, bude odesílatel podle posouzení povahy podání zpravidla vyzván, aby nedostatky podání odstranil, tedy aby k podání připojil svůj elektronický podpis.

**Technické parametry přijímaných datových zpráv:**

1. Datové zprávy jsou přijímány ve formátech:
\*.doc nebo \*.docx (dokument Microsoft World 97 a vyšší)
\*.xls nebo \*.xlsx (dokument Microsoft Excel 97 a vyšší)
\*.ppt nebo \*.pptx (dokument Microsoft Powerpoint 97 a vyšší)
\*.odt (dokument OpenOffice Writer)
\*.ods (dokument OpenOffice Calc)
\*.odp (dokument OpenOffice Impress)
\*.rtf (textový standard RTF-DCA)
\*.txt (prostý text)
\*.pdf (dokument Adobe Acrobat)
\*.zip nebo \*.rar (komprimovaný dokument)
\*.jpg, \*.jpeg, \*.tif, \*.gif (grafický formát)

2. Maximální velikost datové zprávy:
Podle § 5 vyhlášky č. 194/2009 Sb. je maximální velikost datové zprávy dodávané do datové schránky 10 MB.

3. Kontrola datové zprávy:
Datová zpráva nesmí obsahovat škodlivý kód, který může poškodit informační systém datových schránek, údaj v něm obsažený nebo výpočetní techniku držitele datové schránky; na základě § 7 vyhlášky č. 194/20098 Sb. takovou datovou zprávu správce informačního systému datových schránek nepřijme k odeslání, stejně jako datovou zprávu, která není vytvořena v přípustném datovém formátu nebo která převyšuje svou velikost maximální stanovenou velikost.

**Potvrzení o přijetí a doručení elektronického podání:**

Doručení datové zprávy se potvrzuje odesilateli neprodleně zasláním datové zprávy, pokud je orgán veřejné moci schopen z přijaté datové zprávy zjistit elektronickou adresu odesilatele. Součástí zprávy o potvrzení doručení je

a) uznávaný elektronický podpis oprávněného zaměstnance orgánu veřejné moci nebo uznávaná elektronická značka orgánu veřejné moci,
b) datum a čas s uvedením hodiny, minuty a sekundy, kdy byla datová zpráva doručena, a
c) charakteristika doručené datové zprávy umožňující její identifikaci.

 **Postup v případě zjištění škodlivého softwaru u přijaté datové zprávy:**

Pokud byl u datové zprávy zjištěn škodlivý software, není tato zpráva zpracovávána. Je-li možné z přijaté datové zprávy zjistit elektronickou adresu odesilatele, je na tuto adresu zasláno sdělení o zjištění škodlivého softwaru.