



DZIENNIK USTAW RZECZYPOSPOLITEJ POLSKIEJ

Warszawa, dnia 16 stycznia 2018 r.

Poz. 126

ROZPORZĄDZENIE RADY MINISTRÓW

z dnia 27 grudnia 2017 r.

w sprawie dokumentów związanych z czynnościami spółdzielczych kas oszczędnościowo-kredytowych sporządzanych na informatycznych nośnikach danych

Na podstawie art. 3a ust. 4 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2017 r. poz. 2065, 2486 i 2491 oraz z 2018 r. poz. 62 i 106) zarządza się, co następuje:

§ 1. Rozporządzenie określa sposób tworzenia, utrwalania, przekazywania, przechowywania i zabezpieczania, w tym przy zastosowaniu środków identyfikacji elektronicznej, dokumentów związanych z czynnościami, o których mowa w art. 3 ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, zwanych dalej „czynnościami kas”, sporządzanych na informatycznych nośnikach danych.

§ 2. Ilekroć w rozporządzeniu jest mowa o:

- 1) podpisie elektronicznym – należy przez to rozumieć kwalifikowany podpis elektroniczny albo inny podpis elektroniczny oparty na danych identyfikujących podpisującego, zgodny z umową stron, a w przypadku dokumentów wewnętrznych spółdzielczej kasy oszczędnościowo-kredytowej, zwanej dalej „kasą”, zgodny z jej uregulowaniami wewnętrznymi;
- 2) integralności – należy przez to rozumieć właściwość polegającą na tym, że zawartość dokumentu nie uległa zmianie od chwili jego utworzenia.

§ 3. Utworzenie i utrwalenie następuje przez zapisanie w dokumencie elektronicznym danych związanych z jedną lub wieloma czynnościami kas oraz jego opatrzenie podpisem elektronicznym.

§ 4. Dokument w formie dokumentu elektronicznego może być przekazany na informatycznym nośniku danych albo za pośrednictwem środków komunikacji elektronicznej, w sposób gwarantujący integralność przekazywanych danych.

§ 5. 1. Dokument przechowuje się w sposób gwarantujący nienaruszalność jego integralności, zapewniający możliwość odczytania zawartych w nim informacji przez cały okres jego przechowywania oraz możliwość weryfikacji podpisu elektronicznego, którym ten dokument został opatrzony.

2. Jeżeli okres trwałości zapisu na informatycznym nośniku danych określony przez producenta tego nośnika jest krótszy od wymaganego okresu przechowywania dokumentu, wówczas utrwalony na nośniku dokument należy przenieść na inny informatyczny nośnik danych przed upływem gwarantowanego przez producenta okresu trwałości zapisu. Informatyczny nośnik, z którego przeniesiono zapis, podlega modyfikacji w celu uniemożliwienia odtworzenia dokumentu.

3. Po upływie wymaganego okresu przechowywania dokument zostaje usunięty z informatycznego nośnika danych w sposób nieodwracalny. W przypadku upływu wymaganego okresu przechowywania wszystkich dokumentów utrwalonych na informatycznym nośniku danych, nośnik ten podlega modyfikacji w celu uniemożliwienia odtworzenia tych dokumentów.

§ 6. 1. Dokumenty przechowuje się w co najmniej dwóch kopiach, każda na innym egzemplarzu lub rodzaju informatycznego nośnika danych. Sposób przechowywania nośników obydwu kopii powinien zapewniać bezpieczeństwo zapisanych na nich dokumentów.

2. Dokumenty mogą być kopiowane na inny informatyczny nośnik danych jedynie pod nadzorem osób, które zostały uprawnione zgodnie z wewnętrznymi procedurami kas, z zachowaniem zasad bezpieczeństwa obrotu oraz ochrony interesów kas i ich klientów.

3. Każdy informatyczny nośnik danych użyty do przechowywania dokumentów powinien zawierać oznaczenie umożliwiające identyfikację tego nośnika (identyfikator).

§ 7. 1. Dokument uważa się za zabezpieczony, jeżeli w sposób ciągły:

- 1) jest zapewniona jego dostępność wyłącznie dla osób uprawnionych oraz
- 2) jest chroniony przed przypadkowym lub nieuprawnionym zniszczeniem, oraz
- 3) są zastosowane metody i środki ochrony dokumentu, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

2. Zabezpieczenie dokumentów wymaga w szczególności:

- 1) systematycznego dokonywania analizy zagrożeń;
- 2) opracowania i stosowania procedur zabezpieczania dokumentów i systemów ich przetwarzania, w tym procedur dostępu;
- 3) stosowania środków bezpieczeństwa adekwatnych do zagrożeń;
- 4) bieżącego kontrolowania funkcjonowania wszystkich organizacyjnych i techniczno-informatycznych sposobów zabezpieczenia, a także okresowego dokonywania oceny skuteczności tych sposobów.

§ 8. Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Prezes Rady Ministrów: *M. Morawiecki*