



**GENERALNY INSPEKTOR  
OCHRONY DANYCH  
OSOBOWYCH**

*dr Wojciech R. Wiewiórowski*

Warszawa, dnia 18 czerwca 2014 r.

DOLiS-035- 1239 /14

**Prezes Zarządu  
Spółdzielnia Mieszkaniowa**

w związku z uzyskaniem przez Generalnego Inspektora Ochrony Danych Osobowych informacji, z której wynika, iż Spółdzielnia Mieszkaniowa przetwarzając dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.), nie stosuje środków technicznych i organizacyjnych określonych w przepisach tej ustawy, jak również w przepisach wykonawczych wydanych na jej podstawie, w szczególności w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024), tym samym umożliwia dostęp do danych osobowych osobom nieupoważnionym, działając na podstawie art. 19a ust. 1 ustawy o ochronie danych osobowych, zgodnie z którym Generalny Inspektor może kierować do osób fizycznych i prawnych wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych, zwracam się o przedsięwzięcie stosownych środków celem wypełnia ciężących na Spółdzielni obowiązków określonych w ww. aktach prawa.

Generalny Inspektor Ochrony Danych Osobowych uzyskał informację, iż Spółdzielnia Mieszkaniowa przetwarzając dane osobowe w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r., nr 101, poz. 926 z późn. zm.) zwanej dalej także ustawą, zamieszcza na powszechnie dostępnej stronie internetowej spółdzielni dokumenty zawierające dane osobowe – m. in. Sprawozdania Zarządu z działalności, uchwały organów spółdzielni, nie stosując przy tym żadnych środków technicznych i organizacyjnych dotyczących zabezpieczenia tych danych. Każde natomiast przedsięwzięcie związane z przetwarzaniem danych osobowych powinno przebiegać w zgodzie z przepisami obowiązującymi w zakresie przetwarzania danych osobowych. Zasady przetwarzania danych osobowych, określone zostały w przepisach ustawy, jak również w przepisach wykonawczych wydanych na jej podstawie, w szczególności w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29

kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) zwane dalej rozporządzeniem.

Stosownie do treści art. 8<sup>1</sup> ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Dz. U. z 2013 r. poz. 1222) członek spółdzielni mieszkaniowej ma prawo otrzymania odpisu statutu i regulaminów oraz kopii uchwał organów spółdzielni i protokołów obrad organów spółdzielni, protokołów lustracji, rocznych sprawozdań finansowych oraz faktur i umów zawieranych przez spółdzielnię z osobami trzecimi. Zgodnie z ust. 3 wskazanego przepisu statut spółdzielni mieszkaniowej, regulaminy, uchwały i protokoły obrad organów spółdzielni, a także protokoły lustracji i roczne sprawozdanie finansowe powinny być udostępnione na stronie internetowej spółdzielni.

W opinii Generalnego Inspektora Ochrony Danych Osobowych powyższe nie oznacza, że dokumenty zawierające dane osobowe mogą być bez zastosowania żadnych zabezpieczeń, chroniących przed dostępem do danych osobom nieupoważnionym, zamieszczone na stronie internetowej spółdzielni. Dokumenty (takie jak sprawozdania Zarządu, uchwały organów spółdzielni, itp.) zawierające dane osobowe, przed zamieszczeniem na powszechnie dostępnej stronie internetowej powinny zostać wcześniej zanonimizowane w sposób uniemożliwiający identyfikację osób. Natomiast dokumenty zawierające dane osobowe powinny być dostępne jedynie uprawnionym do tego na mocy stosownych przepisów, osobom.

Pomocniczo wskazuję na treść wyroku Trybunału Konstytucyjnego z dnia 15 lipca 2009 roku (sygn. K. 64/2007), w którym Trybunał stwierdził, iż „*W ocenie Trybunału Konstytucyjnego, art. 8[1] ust. 3 usm powinien być interpretowany systemowo, która to wykładnia warunkuje zgodność tego przepisu z art. 51 ust. 1, 3 i 5 Konstytucji, gwarantującym autonomię informacyjną jednostki. Kwestionowany w niniejszej sprawie przepis znajduje się w rozdziale 1[1] usm zatytułowanym „Prawa członków spółdzielni mieszkaniowej”. Zatem konstytucyjnie uprawniona interpretacja art. 8[1] ust. 3 usm nakazuje przypisanie przewidzianych w nim uprawnień jedynie członkom spółdzielni mieszkaniowej. Udostępnianie osobom spoza tego kręgu statutu, regulaminów, uchwał i protokołów obrad organów spółdzielni, a także protokołów lustracji i rocznych sprawozdań finansowych nie znajduje konstytucyjnego uzasadnienia. Tym samym powodowałoby nieuprawnione ograniczenie prawa do ochrony danych osobowych przysługującego w tym przypadku członkom spółdzielni mieszkaniowej. Oczywiście powyższe ustalenia determinują przyjęcie określonych rozwiązań technicznych, które zapewniłyby dostęp do dokumentów zawartych na stronie internetowej spółdzielni mieszkaniowej tylko osobom uprawnionym, a więc członkom spółdzielni (np. system logowania się na stronie za pomocą określonego hasła).*”, LexisNexis nr 2053722

Wskazuję także, że stosownie do art. 36 ust. 1 ustawy o ochronie danych osobowych administrator danych ma obowiązek zabezpieczenia danych m.in. przed ich nieuprawnionym ujawnieniem. Jednym ze środków służących ochronie danych, jest ich szyfrowanie. W szczególności obligatoryjne jest szyfrowanie przesyłanych danych zgodnie z pkt XIII części C załącznika do rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. zatytułowanej „Środki bezpieczeństwa na poziomie wysokim”, wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

W razie przesyłania danych metodą teletransmisji przy użyciu sieci publicznej zawsze istnieje możliwość przejęcia przesyłanych danych przez osobę nieuprawnioną. Istnieje również niebezpieczeństwo ich nieuprawnionej zmiany, uszkodzenia lub zniszczenia. Niezbędne jest zatem

zastosowanie odpowiednich zabezpieczeń, które ochronią przesyłane dane. O tym, jakie środki należy zastosować, administrator danych powinien zdecydować samodzielnie. Może to być protokół szyfrowania danych SSL, jak również inne środki ochrony kryptograficznej, np. szyfrowanie przy użyciu poczty elektronicznej i klucza publicznego odbiorcy.

Powyżej wskazane rozporządzenie określa: sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną; podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych; wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych. Ponadto przepisy powyższego rozporządzenia określają jedynie minimalne wymagania dotyczące zabezpieczenia systemu informatycznego.

Obowiązek właściwego zabezpieczenia danych osobowych z uwzględnieniem kategorii danych objętych ochroną oraz możliwych zagrożeń jest obowiązkiem „dynamicznym”, co znaczy, że nie może być spełniony jednorazowo. Administrator danych jest obowiązany monitorować i oceniać zmieniające się zagrożenia w związku z przetwarzaniem danych osobowych i odpowiednio do zachodzących zmian wykorzystywać, uwzględniając osiągnięcia nauki i techniki, środki techniczne i organizacyjne (A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2007, Wydawnictwo Prawnicze LexisNexis (wydanie III) s. 504). Prawidłowe zaś zarządzanie zasobami informacyjnymi, zwłaszcza w aspekcie bezpieczeństwa informacji, wymaga właściwej identyfikacji tych zasobów oraz określenia miejsca i sposobu ich przechowywania. Wybór zaś odpowiednich dla poszczególnych zasobów metod zarządzania ich ochroną i dystrybucją zależy jest od zastosowanych nośników informacji, rodzaju zastosowanych urządzeń, sprzętu komputerowego i oprogramowania.

Reasumując, administrator danych ma zarówno obowiązek do zorganizowania bezpieczeństwa procesu przetwarzania danych osobowych, w sposób odpowiadający przepisom obowiązującym w zakresie przetwarzania danych osobowych, jak i prawo dokonania tego w taki sposób, który odpowiadał będzie zagrożeniom oraz kategoriom przetwarzanych danych. To administrator decyduje i odpowiada za powyższe i za przetwarzanie danych zgodnie z prawem.

Informuję także, że umożliwienie dostępu do danych osobowych osobom nieupoważnionym, jak również zlekceważenie obowiązku zabezpieczenia danych osobowych przed ich zabránieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem może prowadzić do odpowiedzialności karnej z art. 51 i 52 ustawy o ochronie danych osobowych.

Wskazuję, że zgodnie z art. 19a ust. 3 ustawy, podmiot, do którego zostało skierowane wystąpienie lub wnioski, o których mowa w ust. 1 i 2, jest obowiązany ustosunkować się do tego wystąpienia na piśmie **w terminie 30 dni** od daty jego otrzymania.