

# ***Outsourcing* danych ubezpieczeniowych (w tym danych osobowych)**

**adw. Xawery Konarski**

# Agenda

---

- *outsourcing* czynności ubezpieczeniowych a *outsourcing danych* ubezpieczeniowych
- tajemnica ubezpieczeniowa (zakres przedmiotowy, podmiotowy)
- chmura obliczeniowa jako szczególny przypadek *outsourcingu* danych ubezpieczeniowych

# ***Outsourcing* czynności ubezpieczeniowych ≠ *outsourcing* danych ubezpieczeniowych**

---

- *outsourcing* danych wykonywany również przez inne podmioty niż podmioty wykonujące czynności ubezpieczeniowe (art.19 ust.1 pkt 23 u.d.u.)
- *outsourcing* danych w zakresie niezbędnym do czynności wykonywanych przez pośredników ubezpieczeniowych (art.19 ust.1 pkt 24 u.d.u.)

# Tajemnica ubezpieczeniowa – zakres podmiotowy (1)

---

- osoby zobowiązane do zachowania tajemnicy ubezpieczeniowej:
  - zakład ubezpieczeń
  - osoby zatrudnione w zakładzie ubezpieczeń
  - inne osoby i podmioty, które wykonują czynności ubezpieczeniowe np. na podstawie umów cywilnoprawnych

# Tajemnica ubezpieczeniowa – zakres podmiotowy (2)

---

- tajemnica agenta ubezpieczeniowego (art.13 ust.1 pkt 3 u.p.u.):
  - wszystkie informacje uzyskane w związku z wykonywaniem czynności agencyjnych, dotyczące zakładu ubezpieczeń, drugiej strony umowy ubezpieczenia oraz podmiotu szukającego ochrony ubezpieczeniowej
- wniosek: obowiązek określony w art. 13 ust. 1 pkt 3 u.p.u. przekracza granice dyspozycji art. 19 ust. 1 u. d.u., ponieważ obejmuje także:
  - wszelkie informacje uzyskane w związku z wykonywaniem czynności agencyjnych (np. informacje dotyczące podmiotu poszukującego dopiero ochrony ubezpieczeniowej)

# Tajemnica ubezpieczeniowa – zakres podmiotowy (3)

---

- tzw. „pierwotni adresaci” obowiązku, wyraźnie wskazani w przepisach prawa (art. 19 ust. 1 u.d.u.),
- tzw. „wtórni adresaci” obowiązku tj. podmioty, które uzyskały informację objętą tajemnicą na zasadzie wyjątku (np. podmioty określone w art.19 ust.1 pkt 23 u.d.u.?)
- *ratio legis*:
  - brak rozszerzenia zakresu stosowania wymogów w stosunku do tych podmiotów skutkowałoby osłabieniem poziomu ochrony tego rodzaju informacji, które po „wydostaniu się” poza krąg „pierwotnych adresatów” nie podlegałyby już ochronie (poza ewentualną ochroną na gruncie u.o.d.o.)

# Tajemnica ubezpieczeniowa – zakres podmiotowy (4)

---

- zakaz *outsourcingu* łańcuchowego danych ubezpieczeniowych
  - istota zakazu – dopuszczalność ujawnienia tylko podmiotom wyraźnie wymienionym w art.19 ust.2 u.d.u.
  - konsekwencje praktyczne dla sposobu zawierania umów *outsourcingu* danych ubezpieczeniowych
- problematyka prawna działania *multi-outsourcera*
  - dopuszczalność zestawiania, na różne cele, *outsourcowanych* przez ZU (?)
  - multiagent jako szczególny przypadek *multi-outsourcera* (np. spółka dystrybucyjna i spółki produktowe z grupy ubezpieczeniowej)

# Tajemnica ubezpieczeniowa – zakres przedmiotowy

---

- ochroną wynikającą z art. 19 ust. 1 u. dz. u. objęta jest:
  - całość umowy ubezpieczenia oraz indywidualne dane zawarte w innych dokumentach dotyczących tej umowy
- chodzi tu o dane wynikające ze stosunku cywilnoprawnego umowy, o których mowa w art. 805 k.c.
- zakaz ujawniania danych obejmuje zakaz (wyrok NSA w Warszawie z 5 czerwca 2001 r. III SA 2661/00):
  - ujawniania treści samej umowy (art. 805 k.c.),
  - dokumentu ubezpieczenia (art. 809 k.c.),
  - składki (art. 812 k.c.),
  - informacji pochodzącej od ubezpieczonego (art. 815 k.c.)



# Ochrona danych ubezpieczeniowych w chmurze obliczeniowej

---

- brak szczególnych regulacji w u.d.u.
- zakres stosowania polskich przepisów u.o.d.o.:
  - polskie przepisy nie stosują się do zagranicznych dostawców usługi chmury obliczeniowej (*cloud provider*)
  - użytkownik chmury (administrator danych) odpowiada jednak za środki zabezpieczenia danych podjęte przez dostawcę chmury (*processor*) - art.31 ust.4 u.o.d.o.
  - wniosek: treść art.31 ust.4 u.o.d.o. w sposób „pośredni” wymusza stosowanie polskich przepisów o zabezpieczeniu danych przez zagranicznych dostawców usługi chmury obliczeniowej

# Ochrona danych ubezpieczeniowych w chmurze obliczeniowej

---

- środki zabezpieczenia danych w chmurze obliczeniowej:
  - art.36 ust.1 u.o.d.o. – „*administrator danych jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną*”
  - problem prawny: czy GIODO może żądać np. wyników audytu, właściwej polityki w zakresie *risk assessment* etc. (a więc innych środków zabezpieczenia danych niż wymienione w uodo i rozporządzeniu wykonawczym)?

# IT w ubezpieczeniach – postanowienia umowne w umowach na chmurę obliczeniową

---

- postanowienia umowy pomiędzy dostawcą, a użytkownikiem (zgodnie z rekomendacją Grupy Roboczej art.29):
  - SLA usługi oraz sankcje za ich niedotrzymanie
  - specyfikacja technicznych i organizacyjnych środków zabezpieczenia do których podjęcia jest zobowiązany dostawca usługi
  - zasady podpowierzenia przetwarzania danych przez dostawcę usługi
  - obowiązek informowania użytkownika o zmianach sposobu świadczenia usługi
  - obowiązek informowania użytkownika o wszelkich naruszeniach bezpieczeństwa danych
  - obowiązek informowania użytkownika o otrzymanych przez dostawcę usługi żądaniach udostępniania przechowywanych danych
  - zasady wsparcia administratora (użytkownika usługi) w zakresie wykonywania obowiązków względem podmiotów danych
  - postanowienia dotyczące audytu i monitoringu wykonania usługi
  - postanowienia regulujące obowiązki dostawcy usługi w przypadku rozwiązania umowy

---

Dziękuję za uwagę.

[xawery.konarski@traple.pl](mailto:xawery.konarski@traple.pl)