

## Коментари Телекома Србија а.д. у вези са нацртом Закона о информационој безбедности

1. Мишљења смо да Закон треба да се експлицитније позове на међународно признате стандарде (ИСО 27000 фамилија) како би се искористила већ изграђена инфраструктура сертификације и акредитације у погледу информационе безбедности која постоји код нас. На овај начин би се искористила најбоља светска пракса (која је већ и прихваћена код нас кроз стандард SRPS ISO/IEC 27001).
2. Појмови „аутентичност и непорецивост података“ се обично сматрају делом појма „**интегритет података**“, тако да се ИКТ безбедност бави заштитом поверљивост/тајност, интегритет и расположивост, познате као CIA/ACI (енгл. *Confidentiality, Integrity and Availability*). У том смислу нема потребе да се појмови „аутентичност и непорецивост података“ додатно дефинишу као предмет закона.
3. Законом се ставља акценат на регулисање информационе безбедности државних органа, територијалних аутономија и локалних органа самоуправе док су други сегменти (нпр. пословни, банкарски и др.) остали непокривени, иако се препознају додирне тачке у смислу приступа и поступања с тајним подацима.
4. Законом је предвиђено оснивање Агенције за КБ и заштиту од КЕМЗ. Налазимо да је целисходно регулацијом обухватити и остале области информационе безбедности.
5. Мишљења смо да је појам акредитације погрешно употребљен у Закону. Према важећем Закону о акредитацији („Сл. гласник РС“, бр. 73/2010),

### „Члан 2.

1) акредитација је утврђивање од стране националног тела за акредитацију да ли **тело за оцењивање усаглашености** испуњава захтеве одговарајућих српских, односно међународних и европских стандарда, и када је применљиво, све додатне захтеве дефинисане за поједине области, како би се вршили одређени послови оцењивања усаглашености;“

### Члан 3.

„Акредитацијом се утврђује компетентност тела за оцењивање усаглашености за обављање послова:

- 1) испитивања;
- 2) еталонирања;
- 3) контролисања;
- 4) сертификације производа;
- 5) сертификације система менаџмента;
- 6) сертификације особа.“

Дакле акредитација се односи на тела за оцењивање, што би према хијерархији коју нуди Закон о инф. безбедности значило да би Канцеларија Савета била акредитована да утврђује испуњеност услова који прописује Закон и подзаконска акта односно да ИКТ системи не могу бити акредитовани него сертифицирани за рад са тајним подацима. Сертификацију може да обави акредитовано тело.

6. У члану 9. руковалац ИКТ система може да „акредитује“ свој систем тако што доставља Канцеларији Савета извештај о интерној провери о испуњености услова за акредитовани ИКТ систем. Овим је, налазимо, нарушен принцип независности и објективности провере, јер на овај начин свако може да сачини извештај о интерним проверама и да се „акредитује“ тј. сертифициује.
7. Налазимо да је потребно појаснити даљу намену Уредбе о посебним мерама заштите тајних података у информационо-телекомуникационим системима („Сл. Гласник РС“ бр. 53)?
8. Сматрамо да је целисходно изнети нешто више детаља о ДКМ, а у контексту улоге и обавеза телекомуникационих оператора.

ТЕЛЕКОМ СРБИЈА А.Д.