**Dobre prakse u računarstvu u oblaku**[[1]](#endnote-1)

U slučaju da se određeni podaci ili informacije čuvaju na eksternom serveru, odnosno u oblaku (*cloud*),[[2]](#endnote-2) vaše preduzeće bi trebalo da utvrdi da li neki od tih podataka podležu kontroli spoljne trgovine strateškom robom. U određenim nadležnostima, ukoliko se kontrolisani podaci čuvaju ili preusmeravaju van zemlje, ili dele sa stranim državljanima, to se smatra izvozom i stoga zahteva odgovarajuće odobrenje nacionalnih vlasti. **Vaše preduzeće bi u vezi sa sledećim pitanjima trebalo da konsultuje nacionalne organe nadležne za izdavanje dozvola:**

1. U kojim situacijama se smatra da je tehnologija ili softver „izvezen“ ili „prenet“?
2. Da li se čuvanje podataka u inostranstvu na eksternom serveru, odnosno u oblaku smatra „izvozom“?

**Ako je to primenljivo, vaše preduzeće bi moglo da preduzme sledeće radnje koje bi smanjile mogućnost da kontrolisanim podacima, odnosno informacijama koje se čuvaju „u oblaku“ pristupe neovlašćeni krajnji korisnici:**

* Odredi fizičke putanje i odredišta svih kontrolisanih tehničkih podataka koji su pohranjeni u oblaku kako bi se utvrdilo da li se primenjuju zahtevi u vezi sa izdavanjem dozvola (gde se nalaze podaci, gde se nalaze serveri);
* Od dobavljača usluge (provajdera) zatraži potvrdu kojom se garantuje da će svi kontrolisani podaci biti u celini smešteni na lokalnim serverima u vašoj zemlji i da im neće pristupati strani državljani koji su zaposleni kod dobavljača;
* Čak i da se dobavljač usluge (provajder) na to obaveže, vaše preduzeće treba da posveti dužnu pažnju praćenju kada se kontrolisani podaci čuvaju ili usmeravaju van zemlje, ili učine dostupnim stranim državljanima;
* U slučaju da vaše preduzeće nije sigurno o implikacijama aranžmana o čuvanju podataka na eksternim serverima ili u oblaku, potrebno je da potraži smernice od nacionalnih vlasti i utvrdi da li je potrebna dozvola za transfer kontrolisanih podataka iz oblaka;
* Uspostavi ograničenja u pogledu količine dozvoljenih kopija koje pružaoci usluga čuvanja podataka na eksternim serverima i u oblaku smeju da naprave, i od pružalaca tih usluga zahteva da nakon otkazivanja usluge korišćenja eksternog servera obrišu sve kopije (uključujući i rezervne kopije) takvih podataka;
* Pregleda i izmeni politike i prakse interne usklađenosti (i plan za kontrolu tehnologije, ukoliko je primenljivo);
* Redovno obaveštava i dostavlja ažurne informacije svim zaposlenima u vezi sa pitanjima koja se odnose na čuvanje podataka na eksternim serverima i u oblaku;
* Obezbedi da ugovor o pružanju usluge korišćenja eksternih servera i računarstva u oblaku sadrži tačne odgovornosti svih ugovornih strana koje se odnose na usklađenost, kao i kazne i posledice u slučaju kršenja tih odredaba ugovora; i
* Poveća bezbednost podataka dodavanjem lozinki, prijava i/ili enkripcija za pristup.

1. Prilagođeno i modifikovano iz “Impact of Export Controls on Higher Education & Scientific Institutions,” Georgia Tech University, May 5-7, 2014. [↑](#endnote-ref-1)
2. **Definicija:** ,,Računarstvo u oblaku” predstavlja distribuirano računarsko okruženje koje se implementira preko mreže. Videti, “Impact of Export Controls on Higher Education & Scientific Institutions,” Georgia Tech University, May 5-7, 2014, <http://researchintegrity.gatech.edu/files/Export/2014-conference-presentations/Cloud\_Computing\_and\_Encryption\_Cowperthwait\_Metcalf\_Schlesinger\_Smoak\_Wheeler.pdf>. [↑](#endnote-ref-2)