ZASEBNOST V OBLAKU
PRIVACY IN THE CLOUD

MAG. ANDREJ TOMŠIČ,
INFORMACIJSKI
POOBLAŠČENEC RS

POVZETEK

Javne oblike računalništva v oblaku vzbujajo pomisleke glede varstva osebnih podatkov, ki se kažejo predvsem na področju pogodbene obdelave osebnih podatkov, zavarovanja osebnih podatkov ter izvoza podatkov v tretje države. V prispevku so ti pomisleki podrobneje obravnavani, predstavljeni pa so tudi možni mehanizmi, s katerimi bi lahko okrepili zaupanje v storitve računalništva v oblaku. Zaupanje v te storitve je namreč bistveno za pravno nespornost in praktično sprejemljivost računalništva v oblaku pri izvajalcih, ki jih nimamo pod neposrednim nadzorom.

KLJUČNE BESEDE: ZASEBNOST, OSEBNI PODATKI, RAČUNALNIŠTVO V OBLAKU, ZAVAROVANJE OSEBNIH PODATKOV, IZVOZ OSEBNIH PODATKOV, POGODBENA OBDELAVA OSEBNIH PODATKOV

ABSTRACT

Public cloud computing services raise concerns in terms of personal data and privacy protection, which generally touch upon the questions of contractual processing of personal data, data security issues and transfer of personal data to third countries. The article examines these concerns and puts forward some mechanisms that could foster trust in public cloud computing services. Trust in public cloud services that are out of our direct control is fundamental for legal acceptability of such services and a key enabler for deployment in practice.

KEY WORDS: PRIVACY, PERSONAL DATA, CLOUD COMPUTING, DATA SECURITY, EXPORT OF PERSONAL DATA, OUTSOURCING

UVOD

Zadnjih nekaj letih je vedno več govora o računalništvu v oblaku (angl. cloud computing), ki s seboj prinaša veliko tehničnih, pravnih in drugih vprašanj. V oblak se pospešeno seli čedalje več obdelave osebnih podatkov, kar neizogibno poraja dvome glede skladnosti z zakonodajo na področju varstva osebnih podatkov in zasebnosti. V prispevku bom obravnaval računalništvo v oblaku s stališča varstva osebnih podatkov, pojasnil, zakaj ob tem prihaja do pomislekov s strani nadzornih institucij in varuhov zasebnosti ter podal razmišljanje o mehanizmih, ki bi lahko te pomisleke minimizirali.

KAJ JE RAČUNALNIŠTVO V OBLAKU?

Uvodoma moramo pojasniti, kaj sploh obravnavamo s pojmom računalništvo v oblaku. Gre za storitve računalniške obdelave, programske opreme, hrambe in dostopa do podatkov, ki s strani končnega uporabnika ne zahtevajo fizične lokacije, in konfiguracije sistema, ki zagotavlja storitve. Bistvena značilnost računalništva v oblaku je, da obdelava podatkov ne poteka na vnaprej določenem statičnem mestu, ločimo pa med javnimi, skupnostnimi, zasebnimi in hibridnimi oblaki.

V bistvu ne gre za nek popolnoma nov koncept, saj gre po mnenju nekaterih le za sodobno verzijo modela računalništva iz 60-ih, kjer je bil dostop do računalniških zmogljivosti časovno razporejen. Spletna e-pošta, spletna družbena omrežja ali storitve oddaljene hrambe (varnostnih kopij) podatkov so vse oblike računalništva v oblaku. Gre torej za zunanje izvajanje storitev (angl. outsourcing), pri čemer lahko pri zunanjem izvajalcu dobimo tako gostovanje mrežne infrastrukture, programske in strojne opreme, zmogljivosti za hrambo podatkov in tako dalje (Schneier, 2009). Namen in cilji računalništva v oblaku so predvsem omogočiti dostopnost do računalniških zmogljivosti iz katerekoli lokacije na ekonomičen, prilagodljiv in nadgradljiv način.

POMISLEKI NADZORNIH ORGANOV ZA VARSTVO OSEBNIH PODATKOV IN VARUHOV ZASEBNOSTI

V evropskem prostoru je skrb za zasebnost, natančneje za informacijsko zasebnost (varstvo osebnih podatkov) izdatno urejena v nekaterih pravnih aktivih, med katerimi je treba izpostaviti zlasti *Konvencijo Sveta Evrope* o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov Strasbourg iz leta 1981, *Direktivo 95/46/ES* o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter *Zakon o varstvu osebnih podatkov* (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo ZVOP-1). Vidiki varstva osebnih podatkov, ki se ob uporabi računalništva v oblaku najbolj izpostavljajo, so:

- pogodbena obdelava osebnih podatkov,
- zavarovanje osebnih podatkov in
- izvoz osebnih podatkov v tretje države.

POGODBENA OBDELAVA OSEBNIH PODATKOV

Zakonodaja na področju varstva osebnih podatkov (tako Direktiva kot ZVOP-1) seveda dopušča možnost, da upravljavec osebnih podatkov, torej tisti, ki je opredelil namen in sredstva obdelave, določena ravnanja z osebnimi podatki zaupa drugi osebi – pogodbenemu obdelovalcu. Med ta ravnanja lahko sodijo kakršnakoli dejanja, ki vključujejo osebne podatke – obdelava osebnih podatkov namreč pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje. Tu je treba poudariti, da gre tudi v situacijah, ko pogodbeni obdelovalec sploh ne ve, na koga se podatki nanašajo (npr. nudi zgolj storitev gostovanja prostora za hrambo podatkov), za obdelavo osebnih podatkov. Še več – tudi če upravljavec osebnih podatkov svoje podatke hrani pri zunanjemu ponudniku hrambe in na njegovih diskovnih zmogljivostih hrani svoje podatke v kriptirani, zunanjemu ponudniku hrambe neberljivi obliki, tudi takrat gre za hrambo osebnih podatkov, s tem pa za obdelavo osebnih podatkov in zakonske dolžnosti tako naročnika kot ponudnika storitve. Navedeno poudarjam zato, ker marsikje preberemo, da je za varstvo osebnih podatkov poskrbljeno s šifriranjem podatkov. Šifriranje podatkov je le eden od mehanizmov zaščite osebnih podatkov – v izrazoslovju ZVOP-1 gre za zavarovanje osebnih podatkov (angl. data security), skratka za enega od ukrepov s katerim ščitimo celovitost, zaupnost in razpoložljivost podatkov, varstvo osebnih podatkov (angl. data protection) pa je precej širši pojem. Drugače povedano, podatke imamo lahko odlično »zaklenjene«, pa lahko vseeno pride do kršitve varstva osebnih podatkov – morda nimamo pravne podlage za obdelavo osebnih podatkov, morda jih uporabljamo za nezakonite namene, morda jih predolgo hranimo. Pri računalništvu v oblaku nam zanašanje zgolj na tehnične metode lahko izboljša varnost podatkov, ne moremo pa se s tem izogniti zakonodaji na področju varstva osebnih podatkov.

Če se vrnemo na pogodbeno obdelavo podatkov, gre torej za dopustno prakso, pod pogojem, da so vzpostavljene določene varovalke, med njimi pa je bistveno to, da upravljavec osebnih podatkov lahko računa na določen nivo zavarovanja osebnih podatkov. ZVOP-1

1/ Poleg ustreznosti zavarovanja je danski nadzorni organ izpostavil tudi vprašanja zagotovil pogodbenega obdelovalca, razmerja moči med upravljavcem in pogodbenim obdelovalcem ter zakonske pogoje za izvoz osebnih podatkov v oblak.

tako v 11. členu določa, da sme zunanji izvajalec opravljati posamezna opravila v zvezi z obdelavo osebnih podatkov v okviru naročnikovih pooblastil in osebnih podatkov ne sme obdelovati za noben drug namen. Medsebojne pravice in obveznosti morata urediti s pogodbo, ki mora biti sklenjena v pisni obliki in mora vsebovati tudi dogovor o postopkih in ukrepih, s katerimi bodo podatki zavarovani pred slučajnim ali namernim nepooblaščeno uničevanjem podatkov, njihovo sprememba ali izguba ter nepooblaščeno obdelava teh podatkov (24. člen. ZVOP-1). Na tej točki pa pridemo tudi do glavnega pomisleka varuhov zasebnosti – ali in kdaj lahko zaupamo (zunanjemu) ponudniku računalništva v oblaku?

ZAVAROVANJE OSEBNIH PODATKOV

Informacijska varnost je bistveni del in eno temeljnih načel vseh regulativnih aktov na področju varstva osebnih podatkov. Kot je že bilo pojasnjeno, gre za varovanje celovitosti, zaupnosti in razpoložljivosti osebnih podatkov in s tem zelo pomemben del širšega koncepta varstva osebnih podatkov. Na pomen zavarovanja osebnih podatkov je zelo podrobno opozoril danski nadzorni organ za varstvo osebnih podatkov, ki predvsem zaradi teh pomislekov[1] eni od danskih občin ni dovolil uporabe Google Apps (Datatilsynet, 2011). Ali so naši podatki v oblaku bolje varovani ali ne, ni enostavno vprašanje in nanj ni dopustno pavšalno odgovoriti v smislu, da je nekaj, kar imamo sami pod nadzorom, tudi bolj varno (ENISA, 2009). Kot poudarjajo nekateri avtorji gre predvsem za vprašanje zaupanja (Schneier, 2009). Tako kot moramo zaupati operacijskemu sistemu, strojni opremi, programski opremi, moramo zaupati tudi ponudniku računalništva v oblaku – gre pravzaprav za podobno stvar in le za dodatnega ponudnika, ki ga moramo presojati z vidika zaupanja. Pri zunanjem izvajanju pa je vseeno ena pomembna razlika – če imaš računalniške zmogljivosti pod svojim nadzorom, lahko sam ali s pomočjo drugih poskrbiš za varnost s pomočjo drugih varnostnih mehanizmov (dokumente na svojem računalniku lahko npr. varuješ z varnostnimi kopijami, protivirusnimi programi, če recimo popolnoma na zaupaš posamezni rešitvi, npr. brskalniku ali operacijskem sistemu). Pri zunanjemu izvajalcu pa gre za zaupanje v celoti, kar ne vključuje le zaupanja v varnostne postopke in ukrepe, temveč gre tudi za zanesljivost, dostopnost in stanovitnost obratovanja. Pri lastnem izvajanju se namreč ne bojiš, da bo tvoja diskovna polja kupil neposredni tekmec, da bi moral čez noč plačati (več) za dostop do svojih podatkov in da boš podatke čez noč izgubil, če imaš ustrezne postopke varnostnega kopiranja. Ali – oziroma kdaj – smo pri oblaku lahko v to prepričani? Nikakor ne gre pozabiti tudi na človeški faktor, saj se ljudje kljub jasnim politikam pogosto poslužujemo različnih bližnjic. Če je bilo včasih potrebno vdreti v računalnik zaposlenega za pridobitev zaupnih podatkov, je danes morda dovolj dobiti njegovo gmail geslo, če si je zaupne dokumente posredoval na takšen račun, da bo lahko »delal od doma« (Zittrain, 2009).

Posebne težave pri zagotavljanju pričakovane ravni zavarovanja osebnih podatkov porajajo tudi povezana vprašanja izvoza osebnih podatkov v tretje države, ki (ne) zagotavljajo enake ravni varstva osebnih podatkov kot domača jurisdikcija.

IZVOZ OSEBNIH PODATKOV

Kljub nekaterim konvencijam in premikom k mednarodnim standardom (The Madrid Privacy Declaration, 2009) in enotnemu regulativnemu okviru varstva osebnih podatkov

smo trenutno še vedno soočeni z različnimi režimi in ravnmi varstva osebnih podatkov. Izvoz osebnih podatkov iz držav EU (in držav, ki zagotavljajo podobno raven varstva osebnih podatkov[2]) v tretje države je tako možen le pod določenimi pogoji (ZVOP-1 tako izvoz osebnih podatkov ureja v 2. poglavju, členi 63.-71.) Evropski režim varstva osebnih podatkov se precej razlike od ZDA, od koder prihaja nekaj največjih ponudnikov zunanjega računalništva v oblaku, nekateri medsebojni dogovori, kot je t.i. *dogovor o varnem pristanu* (angl. Safe Harbor) pa naj bi omogočili lažjo izmenjavo podatkov med tema različnima režimoma. Varni pristan omogoča upravljavcem osebnih podatkov, da svoje podatke posredujejo upravljavcem ali pogodbenim obdelovalcem iz ZDA (kot so npr. Google, Amazon ipd.), če so se ta podjetja zavezala k spoštovanju načel varnega pristana (Evropska komisija, 2000). Težava je v tem, da gre v bistvu za princip samo-regulacije in nekateri nadzorni organi za varstvo osebnih podatkov so mnenja, da pri računalništvu v oblaku to ne zadostuje (ULD, 2010) in da bi ponudniki računalništva v oblaku – zaradi prej navedenih pomislekov z vidika zavarovanja podatkov – morali biti dolžni ponuditi močnejša zagotovila (Cavoukian, 2008). Podobno stališče zagovarjajo tudi glede certifikacije SAS 70 Type II, ki so jo npr. opravili Amazon, Salesforce.com, Google in Microsoft, saj se izbor kontrol s strani naročnika in revizorja pogosto ščiti in redko objavlja ter se obenem lahko znatno razlikuje od primera do primera (ULD, 2010).

Kakšna naj bi bila potem ustrezna zagotovila? Nadzorni organ za varstvo osebnih podatkov v nemški zvezni deželi Schleswig-Holstein (ULD) navaja dve možnosti. Prva je uporaba t.i. *zavezujočih poslovnih pravil* (angl. Binding Corporate Rules-BCR), gre pa za formalizirane politike oziroma dogovore s strani določene korporacije glede spoštovanja EU načel varstva osebnih podatkov, te dogovore pa mora potrditi nadzorni organ za varstvo osebnih podatkov iz ene ali več držav EU. EU je pri tem razvila tudi postopek t.i. vzajemnega potrjevanja BCR, pri katerem samo potrjevanje prevzame ena od držav članic, njeno presojo pa potem ostale članice zgolj sprejmejo oziroma potrdijo. BCR so postale precej pogost mehanizem za izvoz osebnih podatkov (npr. kadrovskih podatkov, podatkov o naročnikih) iz EU v tretje države.

Druga možnost pa je *neodvisno zunanje certificiranje* s strani ustrezno usposobljenih organizacij ali združenj. Določene aktivnosti v tej smeri vodi združenje Cloud Security Alliance (CSA), katerega cilj je oblikovati smernice za varno računalništvo v oblaku. Med možne posamezne ukrepe sodi tudi certificiranje rešitev v smislu pridobitve potrdila oziroma certifikata.

Pri preučevanju varstva zasebnosti ob izvozu podatkov v tretje države ne gre pozabiti na vprašanja dostopa do podatkov s strani tretjih oseb, ki lahko zakonito ali nezakonito prestrezajo podatke med uporabnikom in ponudnikom računalništva v oblaku. Pri tem gre lahko tako za državne organe (znani so primeri tajnih programov ameriške NSA), kakor tudi za subjekte zasebnega prava, zato so ustrezna zagotovila toliko pomembnejša.

Enotnega mnenja varuhov zasebnosti trenutno še ni, kljub temu pa je možno zaključiti, da je brez ustrezno zagotovljene ravni varnosti računalništva v oblaku uporaba predvsem javnih oblik računalništva v oblaku tvegana in da bo lahko le z ustreznimi varovalkami mogoče pričakovati pravno nespornost in praktično sprejemljivost tovrstnih rešitev.

2/ Seznam vzdržuje Evropska komisija, dostopen je na naslovu: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

ZAKLJUČEK

V prispevku sem obravnaval bistvene pomisleke varuhov zasebnosti, ki se nanašajo predvsem na zagotavljanje zaupanja v storitve (javnega) računalništva v oblaku. Zavarovanje podatkov pri zunanjih izvajalcih, tako na ravni posameznega ponudnika kot na ravni državnega režima varstva osebnih podatkov, v katerega se podatki prenašajo, je pri varuhih zasebnosti najbolj izpostavljeno vprašanje, zavezujoča poslovna pravila in neodvisno zunanje certificiranje pa se kažejo kot možni mehanizmi za vzpostavitev zaupanja tako pri naročnikih kot pri nadzornih organih za varstvo osebnih podatkov.

VIRI

Cavoukian, A. (2008): Privacy in the Clouds. A White Paper on Privacy and Digital Identity: Implications for the Internet. Information and privacy commissioner of Ontario. Dostopno na: http://www.ipc.on.ca/images/Resources/privacyintheclouds.pdf

Cloud Computing und Datenschutz: Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD). Dostopno na: https://www.datenschutzzentrum.de/cloud-computing/ (objavljeno 18.6.2010).

Datatilsynet, The Danish Data Protection Agency: Processing of sensitive personal data in a cloud solution. Dostopno na: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/ (objavljeno 3.2.2011).

Direktiva 95/46/ES z dne Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov. OJ L 281, 23/11/1995.

ENISA: Cloud Computing Risk Assessment. Dostopno na: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment (objavljeno 20.9.2009).

Evropska komisija: 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215 , 25/08/2000 P. 0007 – 0047.

Konvencija Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Uradni list RS(28. 2. 1994)-MP, št. 3-18/1994 (RS 11/1994)).

Schneier, B.(2009): Cloud Computing. Dostopno na: http://www.schneier.com/blog/archives/2009/06/cloud_computing.html (objavljeno 4.6.2009).

The Madrid Privacy Declaration - Global Privacy Standards for a Global World, 3.11.2009. Dostopno na: http://thepublicvoice.org/madrid-declaration/.

Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju: ZVOP-1).

Zittrain, J. (2009): Lost in the Cloud New York Times. Dostopno na http://www.nytimes.com/2009/07/20/opinion/20zittrain.html?_r=1:(objavljeno 19.6.2009).