CLOUD COMPUTING

KAKO ZAŠTITITI SVOJE PODATKE BEZ ISKAKANJA IZ KONCEPTA „CLOUDA"

Mali Priručnik za
firme i javna tijela

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

CLOUD COMPUTING

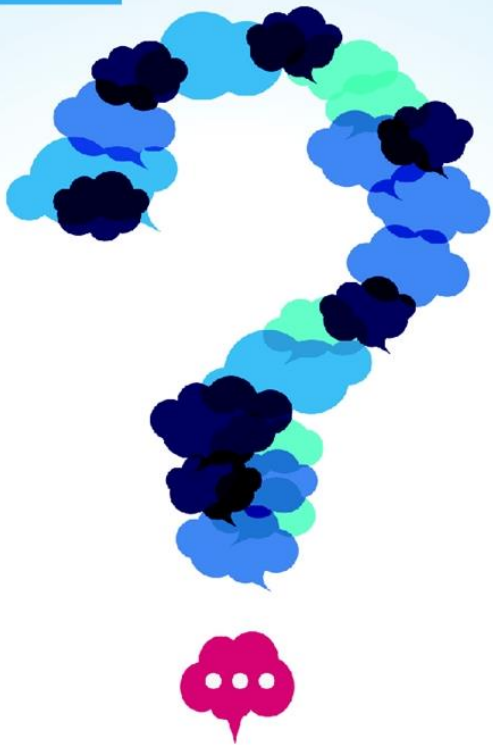
KAKO ZAŠTITITI SVOJE PODATKE BEZ ISKAKANJA IZ KONCEPTA „CLOUDA"

Poduzetnici, kao i javna tijela koja gledaju unaprijed ulažu sve napore da pruže bolje i jeftinije usluge za korisnike i građane. IT tehnologija, a posebno cloud computing, omogućava primjenu inovativnih rješenja za obradu širokog obima aktivnosti učinkovito i relativno jeftino. Međutim, ova tehnologija također podrazumijeva kritične tačke i rizike za privatnost koje treba uzeti u obzir.

Prije ustupanja obrade podataka i evidencija ili uvođenja novih organizatornih modela, trebali biste postaviti sebi nekoliko pitanja i posvetiti posebnu pažnju pri odabiru rješenja koja najbolje mogu osigurati sigurnost svojih institucionalnih i poslovnih aktivnosti.

S ovim Priručnikom, italijansko tijelo za zaštitu podataka pružilo je smjernice za sve korisnike - u pojedinim poduzećima i javnim upravnim tijelima. Naš cilj je utirati put za analizu glavnih pravnih, ekonomskih i tehnoloških problema u području koje se razvija zapanjujućim tempom u cilju poticanja primjerenog korištenja novih alata za isporuku informatičkih usluga.

CLOUD COMPUTING: ŠTA JE TO?



Cloud Computing, ili samo "Cloud", je set tehnologija i mehanizama za upotrebu IT servisa koji olakšavaju pržanje i oslanjanje na software i omogućava pohranjivanje i obradu velike količine podataka putem Interneta.
Ovisno o specifičnoj konfiguraciji, možete pomaći ili pohranu ili obradu podataka (ili oboje) sa svog kompjutera na sistem davatelja usluga. Dodatno, cloud computing dozvoljava koristi od strane kompleksnog servisa bez kupovine visoko-profilnih kompjutera i opreme ili zapošljavanja osoblja da programira i vodi kompleksan sistem.

Sve se može povjeriti (ustupiti) eksternim provajderima za potencijalni dio cijene, pošto se IT izvori za servise koji vama trebaju mogu dijeliti sa drugim klijentima u sličnoj situaciji.

„IT AUTO" ili CLOUD ZA NEUPUĆENE

Opcija 1 – Uradi sam

Ako pojedinac ili firma treba auto, mogu ga dizajnirati, kupiti pojedinačne komponente, sastaviti ga i postaviti radionicu kod kuće ili u sjedištu kompanije sa osobljem specijaliziranim za popravke i održavanje.

Opcija 2 – Idite prodavaču

Možete izabrati da sebi kupite auto i odvezete ga automehaničaru od povjerenja kada je potrebno, možete iznajmiti, zovnuti taxi ili iznajmiti auto sa vozačem. Izbor između ovih opcija ovisi o tome kako planirate koristiti auto, koliko će vam često trebati, na kakav performas ciljate i, na kraju krajeva, koliko novaca imate u novčaniku.

Cloud computing potpada pod opciju 2. Nema ništa sa vožnjom auta koliko sa dobivanjem IT usluge. Rješenja dostupna u „Cloudu" su obično više fleksibilna, učinkovita, podesiva kao i jeftinija neko kućna rješenja. Ipak, mogu sadržavati rizik gubljenja kontrole nad svojim podacima.

Mi obično koristimo cloud tehnologije bez da to znamo. Neki od najpopularnijih email ili word obrade servisa su u „cloudu". Ustvari, većina funkcija dostupnih na novim generacijama mobilnih telefona (npr. smartphone) su bazirane u „Cloudu" – npr. geo-lokacija servisa koja izlistava najbliže prodavnice ili restorane, ili servis koji omogućava da slušate muziku i igrate se online, i mnoge druge funkcije i aplikacije.

RAZLIČIT „CLOUD“ ZA RAZLIČITE POTREBE.

Postoje različite vrste cloud computinga. Raslike su u načinu strukture „Clouda" i kako se podaci obrađuju (interno ili eksterno) i modelima servisa dostupnih klijentima. Svaki tip „Clouda" pokazuje jedinstvene značajke, koje se trebaju pažljivo procijeniti od strane privatnih i javnih tijela prije nego se oslone na servis baziran na „Cloudu".

TIPOVI CLOUDA

Privatni Cloud

„Privatni cloud" je IT infrastruktura - mreža kompjutera koji daju uslugu - koja je najčešće posvećena potrebama jedne organizacije, koja ima infrastrukturu u svojim prostorijama. Alternativno, menadžment je posvećen trećoj strani putem konvencionalnog ugovora za održavanje servera, koji je podložan strogom nadzoru kontrolora podataka.

„Privatni cloud" može se uporediti sa tradicionalnim centrima podataka u kojima se uzimaju dodatne tehnološke mjere u cilju maximalnog iskorištavanja dostupnih resursa i proširivanja tih resursa kada je to potrebno.

Javni Cloud

U „javnom cloudu", IT infrastruktura je u vlasništvu davatelja usluga specijalizirani za davanje servisnih usluga korisnicima, biznismenima ili javnim tijelima; to se postiže dijeljenjem i dostavljanjem, putem Interneta, IT aplikacija, procesorkom snagom i kapacitetom pohrane podataka. Servisima se pristupa putem Interneta,

što podrazumijeva da se prebacuju ili samo podaci ili podaci i njihova obrada na server sistem davatelja usluga.
Dakle, davatelj usluga igra ključnu ulogu u osiguravanju učinkovitosti o poduzetim mjerama za zaštitu informacija koje su njemu povjerene. Zajedno sa svojim podacima, korisnici prenose većinu kontrole nad takvim podacima ako se odluče za „javni cloud".

Drugi tipovi „Clouda„

Postoje drugi tipovi „Clouda" sa miješanim značajkama kao što je „hibridni cloud", gdje se neke usluge daju putem privatne infrastrukture dok se druge usluge daju putem javnog „clouda", i „cloud zajednice", u kojem IT infrastruktura se dijeli sa nekoliko organizacija u svrhu posebne korisničke zajednice.

TRI MODELA CLOUD USLUGA

Cloud Infrastruktura kao usluga - IaaS

„Cloud" davatelj usluga čini dostupnim osnovne hardware i software alate (kao memorijski prostor, operativni sistem, software za vizualizaciju...) na temelju potrošačkog modela; to jest, čini dostupnim daljinski virtualni server na koji se krajnji korisnici (bilo firme ili javna tijela) mogu osloniti da zamijene ili nadopune njihove IT sisteme kako se održavaju u njihovim prostorijama. Ovi davatelji usluga su specijalizirani tržišni operateri i mogu računati na kompleksnu tehnološku infrastrukturu koja se često distribuira na velikom geografskom području.

Cloud Software kao usluga - SaaS

„Cloud" davatelj usluga čini dostupnim, putem Interneta, različite software aplikacije krajnjim korisnicima. Mogu se sastojati od popularnih uredskih aplikacija koje se dostavljaju putem Web-a, kao proračunske tabele ili word obrada, IT protokol i pravila pristupanju aktima, mailing liste i zajednički kalendari do visoko profiliranih email usluga.

Cloud platforma kao usluga - PaaS

„Cloud" davatelj usluga čini dostupnim napredne opcije razvoja softwarea da bi ispunio određene posebne zahtjeve klijenta. Ovaj tip usluge obično se usmjerava na tržišne operatere koji ga koriste za razvoj vlastitih kao i finansijskih, računovodstvenih ili logističkih aplikacija – ili za njihovu vlastitu upotrebu ili za davanje usluga trećoj strani.
Opet, usluge dostupne od strane davatelja usluga čine gotovo nepotrebnim da se krajnji korisnici opreme sa posebnim ili dodatnim hardware-om ili software-om.

PRAVNI OKVIR

MEĐUNARODNI IZAZOV

Cloud tehnologija se razvija bržim tempom nego zakonodavstvo – ne samo u Italiji nego u cijelom svijetu. Ne postoje ažurirani regulatorni okvir u privatnom ili javnom sektoru i kaznenom pravu koji će uzeti u obzir sve inovacije vezane za cloud computing, kako bi osigurali odgovoarajuće sigurnosne mjere u vezi sa pravnim pitanjima koja mogu proizaći iz usvajanja obrade distribuiranih podataka i za servisa pohranjivanje. Na primjer, europsko zakonodavstvo o zaštiti podataka datira iz 1995. Neke korisne inovacije su predstavljene u okviru zakonodavstva Telekoma nazvan „Telekom paket", i Sastoje se iz Direktive 2009/136 – koja je izmjenila e-privacy Direktivu iz 2002. i čija je transpozicija u toku od strane zemalja članica EU. Mjere naložene u novom pravnom okviru uključuje obavezu za telefonske i internet kompanije da obavijeste nadležno tijelo i (pod određenim uvjetima) korisnike koji su trpili kršenje svojih prava, gubitak ili neželjeno objavljivanje podataka koji se obrađuju u sklopu ponuđene usluge.

Dodatna ključna izmjena u cijelom elektronskom komunikacijskom sektoru – uključujući i cloud computing - očekuje se do 2014. kada će novi opći Propis o zaštiti podataka (COM(2012)11), predložen od strane Europske komisije, stupiti na snagu. Novi Propis će uvesti iste propise u cijeloj EU, sa osvrtom na treće zemlje, što znaci da će italijanski Zakon o zaštiti podataka biti prerađen od početka.

Sa ove tačke gledišta, nadamo se da će doprinijeti manje kompleksnoj i manje rizičnoj upotrebi usluga koje su bazirane na cloud computingu.
Jedan od ključnih inovacija je reformacijski paket koji primorava kontrolore podataka (banke, osiguravajuće firme, zdravstvene agencije, lokalne vlasti, itd.) da imaju obavezu da prijave kršenje sigurnosnih mjera koje se odnose na lične podatke. Pojedinci u pitanju biće, bez odgađanja, obaviješteni o gubitku i/ili krađi njihovih podataka, u odgovarajućim slučajevima.

ZAKONI O PRIVATNOSTI I CLOUD – HRANA ZA MISLI

Do sada, usklađeno domaće i međunarodno zakonodavstvo je prihvaćeno kako bi se omogućilo upravljanje cloud computingom bez ugrožavanja inovacija i razvojnog potencijala IT cloud-a, preduzeća i javna tijela trebaju voditi računa u određivanju rizika koji rezultiraju promjenom na usluge bazirane na cloud-u – uključujući pitanja zaštite ličnih podataka. Ovo se takođe primjenjuje na tzv. „centralna tijela za nabavku", odnosno tijelo zaduženo za kupovinu u ime nekoliko javnih tijela uprave.
Kada javno upravno tijelo ili preduzeće se ponaša kao „kontrolor podataka", i premjesti dio ili sve svoje operacije obrade u vezi ličnih podataka na „Cloud", treba da imenuje provajdera cloud usluga kao „obrađivača podataka".
To znači da će klijent uvijek morati provjeravati kako se, bilo koji podaci koji su preneseni na „cloud", koriste i pohranjuju: klijent, kao kontrloror podataka, također će biti odgovoran za bilo koja kršenja izvršena od strane provajdera.

Međutim, klijent manjeg razmjera kao SME (?) ili lokalno tijelo, bi našli za zatežavajuću okolnost da pregovaraju o odgovarajućim uslovima za upravu podataka baziranih na „cloudu"; ipak, tvrdnjom da je klijent bio u nemogućnosti da pregovara strožije ugovorne uslove nadzorne mehanizme, neće biti dovoljno da opravda kršenje (?). Uistinu, klijent „Cloud" baziranih servisa, može se prijaviti i drugim provajderima, koji si mogu priuštiti jaču zaštitu posebno vezanu za zaštitu podataka. Osim toga, italijansti Kodeks (Zakon) o zaštiti podataka propisuje da je kontrolor podataka ovlašten da nadzire (kontroliše) postupanje obrađivača podataka provjerom da li je obrađivač u skladu sa uputama s obzirom na lične podatke koji se trebaju obraditi.

Protok podataka izvan EU

Italijanski Zakon o privatnosti uključuje detaljna pravila za prijenos podataka izvan EU i, u principu, zabranjuje „čak i tranzitni" prijenos ličnih podataka u zemlje koje nisu članice EU ako odgovarajući nivo zaštite nije osiguran od strane pravnog sistema tranzitne zemlje i/ili finalne destinacije podataka.
To često može biti slučaj ako se oslanjate na javne „cloud" usluge naspram privatnih i/ili hibridnih „cloud" usluga.

Dakle, kontrolor podataka – obično klijent koji kupuje usluge zasnovane na „cloud-u"- mora da uzme u obzir i njegove odredbe gdje će se podaci pohranjivati i kakvi se procesi obrade očekuju u inozemstvu. Na primjer, prijenos podataka u SAD može biti lakši ako je pružatelj „cloud" usluga potpisao program zaštite podataka poput tzv. „Safe Harbor" – bilateralni EU-SAD ugovor koji uključuje zajednička sigurnosna pravila za dozvolu prijenosa ličnih podataka kompanijama osnovanim u SAD-u.
Ograničenja prekograničnih tokova podataka također imaju utjecaja na „intra-group" tokove podataka u multinacionalnim okruženjima; ovdje, dostupnost otpornih „obavezujućih pravila" za zaštitu ličnih podataka može dopustiti prijenos podataka poštujući privanost nosioca podataka.

Sigurnost podataka

Kontrolor podataka treba da osigura da su tehničke i organizatorne mjere na mjestu radi smanjenja rizika uništavanja ili gubljenja podataka (čak i nehotično), radi pristupa neovlaštenih lica ili nezakonite obrade na način koji nije u skladu sa svrhom u koju su prikupljeni,

ili da se mogu mijenjati radi neovlaštenih ili nezakonitih radnji.
Na primjer, klijent mora osigurati da su podaci uvijek „dostupni" – što znači, da im se može pristupiti u svako doba – i da su „povjerljivi" – što znači, da im samo ovlaštena lica mogu pristupiti.
Da bi se podaci osigurali, moramo se fokusirati, ne samo na to kako se pohranjuju, nego i kako se prenose – npr. – putem enkripcijske tehnologije.

Prava nosioca podataka

Bilo koje javno upravno tijelo ili preduzeće koje odluči da upravlja ličnim podacima korisnika i kupaca putem „cloud" usluge ne smije zaboraviti da italijanski Zakon o privatnosti omogućuje nosiocima podataka, odnosno, pojedincima na koje se podaci odnose – da ostvaruju određena prava.
Na primjer, nosioci podataka imaju pravo da znaju koje podatke o njima ima javno tijelo ili preduzeće; u koju svrhu(e) se podaci prikupljaju; i kako se obrađuju.

Mogu podnijeti razumljivu kopiju njihovih ličnih podataka da bi se njihovi podaci ažurirali, ispravili i dopunili.
U slučaju kršenja prava, nosioci podataka mogu svoje podatke blokirati, izbrisati ili anonimizirati.
Kako bi bili u skladu sa ovim zahtjevima, klijent usluge bazirane na „cloudu" – pošto je kontrolor podataka – mora adekvatno nadzirati, ne samo pružatelja usluga, nego i sve pod-obrađivače čije usluge pružatelj usluga možda odluči koristiti.

PROCJENA RIZIKA, TROŠKOVA I KORISTI

Pri odabiru tipa „clouda" i modela usluga koji najbolje odgovara vašim potrebama, morate biti posebno oprezni.
Ovo je posebno važne ako se odlučite za javni „cloud", gdje se u osnovi sva obrada ustupa i vaša najvrijednija informacija vam je izvan vaše direktne kontrole. Koncep „clouda" možda zvuči nejasno i „virtuelno"; u suštini, „cloud" tehnologije omogućavaju rukovanjem materijalnih usluga kao što su lanac dostave kompanije, popis registra lokalnih vlasti, liječničke preglede i lab. testove, online bankarstvo i još puno toga. Niko ne bi ostavio svoj novčanik sa svojim ličnim dokumentima i platom nekom Tomu, Dicku ili Harryu; niti biste povjerili svoju bankovnu knjižicu ili prodajni ugovor nepoznatom knjiigovođi koji vam je obećao da će te uštedjeti više ako uradite „ovako" – bez da prvo provjerite kako će te vrijedne dokumente čuvati ili koristiti.

Prema tome, „čuvanje" ne bi trebala biti jedina varijabla pri vašem odabiru. Postoji nekoliko velikih pružatelja usluga „cloud computinga"; u osnovi sve ostale kompanije koje nude cloud usluge i infrastrukturu pomažu ovakvim vođama. To znači da pregovaračka moć pojedine kompanije ili malog javnog upravnog tijela je znatno smanjena, tako da je teško okrenuti tehnološku fleksibilnost u ugovornu fleksibilnost. Tada biste htjeli udružiti snage sa ostalim javnim tijelima i/ili kompanijama sa istim potrebama (npr. putem vaših trgovinskih ili sektorskih udruga) da biste izgradili svoju pregovaračku moć. Prije odlučivanja za određeni tip „clouda", trebate provjeriti za količinu i tip informacija koji će se ustupiti – da li će to uključiti lične podatke uz osjetljive lične podatke, ili će se sastojati od informacije koja je ključ za vaš posao/aktivnosti, kao i povjerljivi ili patentirani projekti ili industrijske tajne?

Trebate procijeniti moguće rizike i posljedice svojih izbora. Istina je da su klijenti često u nemogućnosti da pregovaraju izmjene na „Uslove usluga" pružatelja; ipak, mogu sigurno izabrati drugog pružatelja. Cloud pružatelji također se koriste prilikama pružajući „privacy-friendly" (drugarska privatnost) ugovorne klauzule i/ili oslanjajući se na prijašnje neovisne certifikate o usklađenosti sa EU zakonima o zaštiti ličnih podataka. Ima nekoliko osnovnih pitanja da se postave da biste mogli procijeniti uticaj ovih tehnologija na vašu kompaniju / vaše javno tijelo u smislu troškova i organizatornih rješenja.

SIGURNOST

Koje sigurnosne mjere je pružatelj postavio da bi zaštitio podatke?

Pružatelj „cloud" usluga može često računati na sisteme zaštite od virusa, napada hackera ili drugih IT opasnosti koje su puno efektivnije nego one koje si korisnik pojedinačno može priuštiti. Međutim, trebate utvrditi koje su mjere postavljene od vašeg pružatelja usluga. Prije odlučivanja za svog cloud partnera, imajte na umu da možete izgubiti svoju direktnu, ekskluzivnu kontrolu nad svojim podacima ako ih date udaljenom pružatelju.

ULOGE I ODGOVORNOSTI

Ko ustvari pruža uslugu koju ćete kupiti?
Da li je to kompanija ili grupa kompanija?

Usluga koju izaberete može biti krajnji rezultat „transformacijskog lanca" usluga koje su kupljene

od drugih pružatelja usluga od onih sa kojima imate ugovor.
Ako je lanac posebno dugačak ili kompleksan, nećete biti u poziciji da znate ko od mnogih pružatelja može pristupiti kojim podacima.

DOSTUPNOST USLUGA I OPORAVAK OD NESREĆE

Ako je internet konekcija prekinuta ili slaba, možete li koristiti usluge koje trebate bez korištenja clouda?
Koliko je potrebno za povratak usluge? Da li postoji plan za oporavak od katastrofe za vaše ključne usluge?

Virtuelne usluge bi se mogle degradirati na praćenje IT napada ili tokom saobraćajnih špica, i mogle bi biti prekinute zbog izvanrednih događaja ili kvarova koji bi učinili podatke privremeno nedostupnim – ako ne postoje odgovarajuće sigurnosne mjere za mrežnu konekciju.
Dakle, trebate pažljivo razmisliti kako će na vašu kompaniju / vaše javno tijelo utjecati kvar usluge, bez obzira na njegovo trajanje, s obzirom na troškove (direktne i indirektne) koje će te morati snositi ako podaci ne budu dostupni i unaprijed postavit plan oporavka sa svojim pružateljem cloud usluga.

POVRAT PODATAKA

Mogu li se podaci na cloudu izgubiti ili uništiti? Prirodne katastrofe ili cyber napadi mogu potkopati radnje nekih centara sa podacima.

Posebno je važno da se možete osloniti na procedure povrata podataka i procjenu finansijskog i organizatornog utjecaja gubitka i/ili brisanja bilo kojih podataka koji su samo dostupni na cloudu.

TAJNOST / POVJERLJIVOST

Postoje li mjere tajnosti zaštite za naše podatke ako konkurent nudi iste usluge bazirane na cloudu?

Pružatelju obrađuju podatke pojedinaca i organizacija koje mogu imati različite ili sukobljene/suprotstavljene interese i zahtjeve. Dakle, trebate procijeniti sigurnosne mjere koje se pružaju da bi se osigurala tajnosi informacija koju povjeravate cloudu.

LOKACIJA SERVERA

U kojoj se zemlji, podaci koji su preneseni, na kraju čuvaju?

Možete li se odlučiti da se oslonite samo na servere koji su smješteni na državnoj teriroriji, ili u EU zemljama?

Lokacija pohranjivanja/obrade podataka direktno utiče i na primjenjivo pravo – u slučaju sporova između klijenta i pružatelja – i na državna pravila primjenjiva na obradu, pohranjivanje i sigurnost podataka.

Ovo će osigurati veću transparentnost u odnosu klijent – pružatelj usluga.

Dodatno, ne treba zaboraviti da zakoni o privatnosti dopuštaju samo „iznos" podataka iz EU pod određenim uslovima i ako su provedene adekvatne zaštitne mjere za nosioca podataka u usporedbi zaštite pod EU zakonodavstvom

Dakle, usluga bazirana na cloudu može sadržati nepredviđene dodatne troškove koji rezultiraju iz korisnikove ograničene kontrole nad svojim podacima, ili – što je puno vjerovatnije - zbog državnih i međunarodnih sporova.

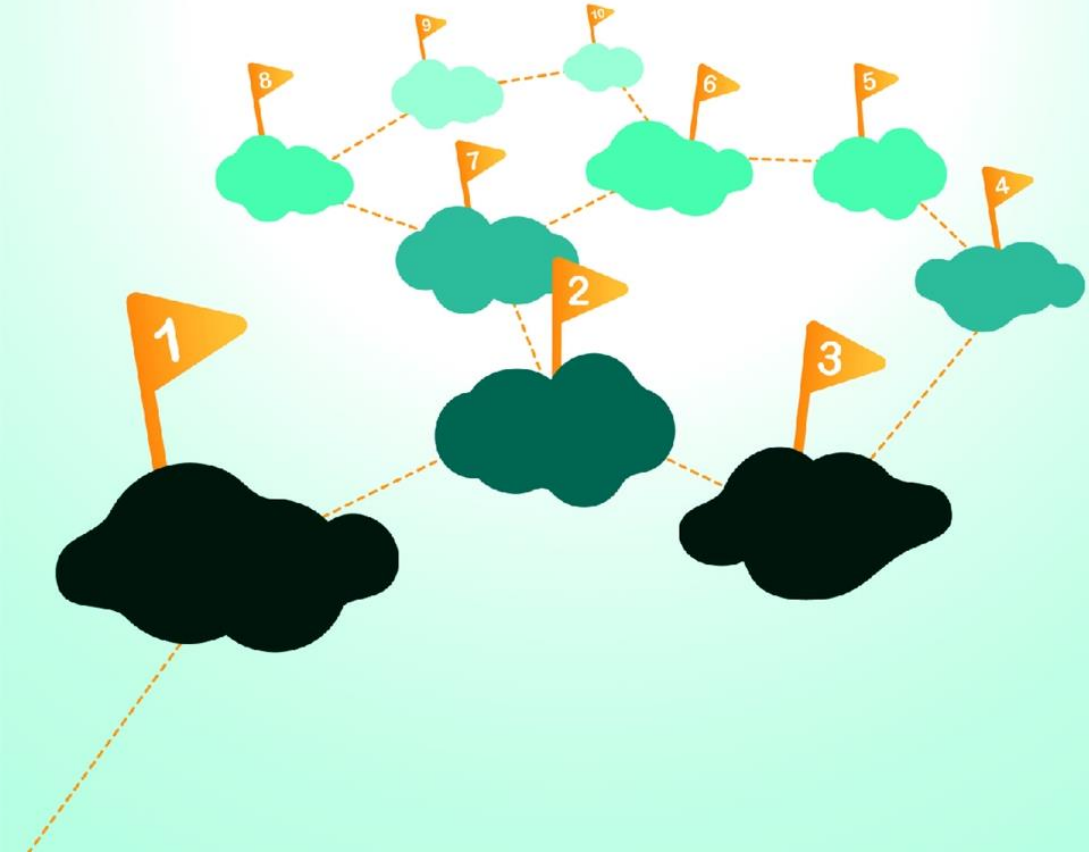
PRIJENOS

Da li se pružatelj cloud usluga oslanja na vlasničku tehnologiju? Mogu li se podaci lako izvesti?
U nekim slučajevima, činjenica da se pružatelj cloud usluga oslanja na vlasničku tehnologiju može za klijenta otežati prijenos podataka i dokumenata među različitim cloud sistemima ili da razmjenjuju informacije sa tijelima koja koriste cloud usluge od različitih pružatelja, što bi značilo da prenosivost podataka i/ili interoperabilnost može biti ugrožena. Ovo je scenario koji može rezultirati u komplikacijama poslovnih strategija.
Na primjer, pružatelj cloud usluga može inicijalno dati vrlo primamljivu ponudu klijentu uključujući odgovarajuće mjere za zaštitu podataka; uzimajući klijenta pružatelj može naknadno promijeniti uslove usluga u svoju korist na pretpostavci da će klijent biti obavezan da prihvati nove uslove pošto mu je praktično nemoguće lako prebaciti podatke drugom pružatelju i okončati ugovor.

OSIGURANJE

Ako se utvrdi da se desilo kršenje podataka ili su podaci nestali, može li pružatelj osigurati brzu otplatu štete?
Zbog nedostatka jasnih propisa, može se pokazati teškim i skupim dobiti odgovarajuću kompenzaciju u slučaju štete od kršenja podataka, gubitka podataka ili (privremenog) prekida usluge. Dostupnost osiguravajuće police i/ili pojednostavljenog mehanizma za rješavanje (međunarodnih) sporova može se pretvoriti u dodanu vrijednost za male korisnike.

DESET PRAVILA
ZA DOBRO UPUĆENE



1

PROVJERITE KOLIKO JE POUZDAN VAŠ PRUŽATELJ

Korisnici trebaju ustanoviti koliko je iskusan, vješt i pouzdan njihov pružatelj prije nego što prenesu većinu svojih vrijednih podataka u cloud; trebaju uzeti u obzir svoje poslovne ili institucionalne zahtjeve, tip i količinu informacija koje će biti premještene u cloud, kao i rizike i sigurnosne mjere. Ovisno od, između ostalog, tipa usluga koje se pružaju i važnosti podataka, korisnici trebaju procijeniti korporativnu strukturu pružatelja; njegove reference; pravne zaštitne mjere za osiguravanje tajnosti podataka skupa sa mjerama na licu mjesta radi sprješavanja neočekivanih kvarova. Dodatno, korisnici trebaju ispitati kvalitetu usluge konekcije na koju se pružatelj oslanja u skladu sa njihovim kapacitetom i pouzdanošću.

Korisnici također trebaju razmotriti da li pružatelj zapošljava iskusno osoblje, koliko je adekvatna IT i komunikacijska infrastruktura pružatelja i do kojeg omjera pružatelj prihvata odgovornost za štete – što treba unaprijed eksplicitno postaviti u uslovima o uslugama – u slučaju sigurnosnih kršenja i/ili kvarova.

BIRAJTE USLUGE SA POJAČANOM PRENOSIVOŠĆU PODATAKA

Klijenti trebaju birati cloud computing usluge koje se oslanjaju na otvorene formate i standarde za smještajne prijenose među cloud sistemima pod upravom različiti pružatelja.
Prenosivost podataka znači da možete povući podatke iz servisa bez dodatnih troškova i neugodnosti koje je teško unaprijed predvidjeti.

Dodatno, ovo će smanjiti rizik da pružatelj izmijeni ugovorne uslove cloud usluge jednostrano protiv klijenta koristeći svoju jaču pregovaračku moć.

OSIGURAJTE DOSTUPNOST PODATAKA KAD GOD VAM JE TO POTREBNO

Klijenti trebaju zahtijevati da njihov ugovor sa pružateljem uključuje jasne, adekvatne sigurnosne mjere o dostupnosti i performansama cloud usluga.

Biranjem usluge koja ne pruža adekvatne i stalne sigrunosne mjere tajnosti mogu znatno uticati ne samo na cloud klijenta nego i na nosioca podataka – mislite na javna upravna tijela ili na bilo koju kompaniju koja pruža usluge trećim licima. Zbog toga, kontrolor podataka – koji je obično klijent clouda – mora osigurati da može imati kopiju bilo kojeg podatka premještenog na cloud bez dodatnih troškova; ovo je posebno odgovarajuće ako se gubitak i/ili nedostupnost takvih podataka pokaže ozbiljno štetnim ne samo za finansije i/ili imidž kontrolora; mislite na visoko osjetljive informacije kao što su zdravstvene ili sudske informacije ili bilo koji podaci o poreznom ili ličnom dohotku.

4

BIRAJTE KOJI PODACI TREBAJU BITI PREBAČENI NA CLOUD

Neki dijelovi informacija, po svojoj samoj prirodi zahtijevaju specifične sigurnosne mjere: to je slučaj sa informacijama zaštićenim industrijskim pravilima tajnosti, kao i osjetljivi podaci kao što su informacije vezano za zdravlje, etničko porijeklo, političko mišljenje ili sindikalno članstvo. Pošto premještanje podataka na cloud, u svim slučajevima, smanjuje korisničku direktnu kontrolu nad takvim podacima, koji su izloženi (ponekad teško predvidivim) rizicima gubitka ili nezakonitog pristupa, korisnici trebaju odgovorno procijeniti da li da se oslone na usluge cloud computinga (posebno javnih cloud usluga) ili da pribjegnu drugim tipovima izmještanja podataka ili čak da nastave sa obradom podataka „u kući".

5

NIKAD NE GUBITE SVOJE PODATKE IZ VIDA

Korisnici trebaju uvijek pažljivo razmotriti tipove ponuđenih usluga i provjeriti da li je pružatelj, koji je ugovorna stranka, će stvarno posjedovati podatke ili da je pružatelj u stvari predstavnik usluge ili se oslanja na tehnologije omogućene od trećih strana. To se može desiti, na primjer, sa cloud aplikacijom gdje se

pružatelj usluge obrade podataka oslanja na uslugu pohranjivanja kupljenu od treće strane: to će dovesti u pitanje klijentove podatke koji su u vlasništvu fizičkih sistema treće strane.
Prema tome, da bi izmjenili kvalitetu cloud usluga mora se ustanoviti ko radi tačno šta od svih tijela uključenih u davanje tih usluga.

6

TREBATE POZNAVATI FIZIČKU LOKACIJU SVOJIH PODATAKA

Važno je za korisnike da znaju da li se njihovi podaci obrađuju na serverima u Italiji, u EU ili u zemlji ne-članici EU.
Ova informacija može biti ključna u utvrđivanju jurisdikcije i primjenjivog prava u slučaju sporova između korisnika i pružatelja usluga;
iznad svega, osnovno je da provjerite zaštitu koja se nudi podacima. Prenosom podataka u zemlje gdje nema adekvatnih sigurnosnih mjera u smislu sigurnosti i tajnosti, može učiniti obradu ličnih podataka nezakonitim i učiniti nepopravljivu štetu institucionalnim aktivnostima javnog tijela kao i poslovanju kompanije.
Prije prenosa podataka na cloud i dopuštanju prenosa podataka u zemlje ne-članice EZ, korisnici trebaju provjeriti da li se ovaj prenos dešava u skladu sa sigurnosnim mjerama postavljenim u italijanskom i EU zakonodavstvu o zaštiti ličnih podataka.
Na primjer, ako je pružatelj SAD kompanija, trebate provjeriti da li je član Safe Harbor ugovora – koji uključuje pravila zaključena prema EU institucijama da bi omogućili obradu ličnih podataka.
Takođe je od pomoći provjeriti da li pružatelj cloud usluga izvan EU je svoje sigurnosne procedure i procedure obrade podredio specifičnim certifikatima kao onima regulisanim

ISO sigurnosnim standardima.
Dodatno, trebate provjeriti da li ugovori o izmještanju podneseni od pružatelja uključuju „standardne ugovorne klauzule" posebno odobrene od Europske komisije za prijenos podataka u treće zemlje.

7

BUDITE UPOZORENI NA VAŠE USLOVE PRUŽANJA USLUGA

Važno je procijeniti da li su postavljeni uslovi pružanja usluga u cloud ugovoru odgovarajući; to je istina, posebno za obaveze i odgovornosti primjenjene na gubitak i/ili neovlašteno objavljivanje podataka čuvanih u cloudu kao i za mehanizme za povlačenje iz usluge i premještanje na drugog pružatelja.
Poseban naglasak treba se staviti na specifikaciju jasnih standarda kvalitete sa odgovarajućim kaznama, tako da je pružatelj odgovoran za nepouzdanost kao i za posljedice posebnih događaja kao što su nedozvoljen pristu, gubitak podataka, nedostupnost zbog kvara i sl.
Da bi ste bili sigurni, provjerite da li su po-izvođači uključeni u pružanje sloud usluga i/ili obradu podataka.

8

PROVJERITE KOLIKO DUGO I NA KOJI NAČIN SE PODACI ZADRŽAVAJU

Prije oslanjanja na cloud usluge, trebate istražiti pružateljevu politiku vezano za zadržavanje podataka na cloudu i osigurati se da je ista utvrđena i ugovorom. Ako zakon

ne propisuje brisanje kontrolorovih podataka istekom ugovora, trebate ustanoviti krajnji rok pružatelju (=obrađivaču podataka) da izbriše sve podatke koji su mu povjereni. Pružatelj mora osigurati da se podaci neće čuvati nakon isteka takvog roka ili kršenja onoga što je eksplicitno dogovoreno sa klijentom. U svim opcijama, svi se podaci moraju čuvati u skladu sa svrhom i dogovorom koji je utvrđen.

9

ZAHTJEVAJTE ADEKVATNE SIGURNOSNE MJERE

U cilju zaštite tajnosti podataka, trebate razmotriti postavljene sigurnosne mjere od strane pružatelja cloud usluga.

Uopćeno govoreći, izbor bi trebao biti pružatelj koji se oslanja na sigurno pohranjivanje podataka i mehanizme prijenosa zasnovani na enkripciji – posebno ako se obrađuju visoko osjetljive informacije – zajedno sa pouzdanim mehanizmima za identifikaciju tijela kojima je omogućen pristup.

ADEKVATNO OBUČITE OSOBLJE

Osoblje klijenta i pružatelja treba biti adekvatno obučeno ukoliko im je zadatak obrada podataka putem cloud computing usluga kako bi smanjili rizike neovlaštenog

pristupa, gubitka podataka i – vjerovatnije – nezakonitih radnji obrade. Obuka treba uključivati tehničke informacije da omogući edukovan odabir cloud tehnologija sa praktičnim koracima obrade kao što je postavljanje podataka na cloud i obrada takvih podataka. Zaštita podataka može biti ugrožena ne samo ako se osoblje ponaša nepošteno ili nepravedno, nego i ako naprave trivijalne greške ili se radi traljavo ili nemarno.

JOŠ NEŠTO O OBRADI U LIČNU SVRHU ILI U SRVHU DOMAĆINSTVA

Italijanski zakon o privatnost se ne primjenjuje na pojedinca koji obrađuje lične podatke u lične svrhe i ne objavljuje takve podatke na Internetu ili ne objavljuje takve podatke sistematski nekolicini pojedinaca.

Ipak, treba podsjetiti da se od pojedinaca takođe očekuje da čuvaju lične podatke sa dužnom pažnjom tako da gubitak takvih podataka ne naškodi drugim pojedincima.
Novi uređaji mobilne tehnologije kao smartphones i tableti imaju značajan kapacitet memorije i obično se oslanjaju na nezaštićene cloud usluge koje dozvoljavaju upotrebu za privatne i profesionalne svrhe – što povećava rizik gubljenja kontrole nad nečijim ličnim podacima.
To znači da trebate čuvati svoje IT uređaje sa pažnjom čak ako ih koristite za ličnu upotrebu; takođe trebate osigurati da treća lica ne mogu pristupiti – pa ni slučajno – ličnim podacima na tim uređajima.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

ITALIAN DATA PROTECTION AUTHORITY

Piazza di Monte Citorio, 121
00186 Rome - Italy
phone +39 06 696771
fax +39 06 696773785

For additional info:
Ufficio per le relazioni con il pubblico
(Front Desk)
Mon-Fri 10-13 on location
or call +39 06 696772917/9
e-mail: urp@garanteprivacy.it

Edited by Servizio relazioni
con i mezzi di informazione
(Media and Outreach Service)

www.garanteprivacy.it

Printed by IAG Mengarelli - June 2012