KOMISIONERI PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË DHËNAVE PERSONALE

UDHËZUES PËR MBROJTJEN E TË DHËNAVE PERSONALE NË SHËRBIMET CLOUD COMPUTING

Tiranë 2014

Udhëzues për Mbrojtjen e të Dhënave Personale në Shërbimet "Cloud Computing"

Zhvillimet në teknologjinë e informacionit janë përshpejtuar. Teknologjia po bëhet gjithnjë e më e fuqishme, e thjeshtë për t'u përdorur dhe gjithnjë e më pak e kushtueshme. I tillë është dhe shërbimi i *cloud computing* si një nga revolucionet më të mëdha teknologjike të shfaqur kohët e fundit.

Metodat që përdoren për të mbledhur dhe përpunuar të dhënat personale janë sofistikuar vazhdimisht. Duke përdorur internetin mund që lehtësisht dhe pa qenë në dijeni (ose pa u paralajmëruar) të këtij fakti të mbeten të ashtu-quajtura gjurmë elektronike.

Zhvillimet kanë bërë që teknologjia të mund të përdoret në një mënyrë që përfshin një ndërhyrje të pajustifikuar në integritetin personal. Në këto kushte individi ka të drejtë të mbrohet nga shoqëria kundër shkeljeve të tilla të integritetit.
Në të njëjtën kohë, nevoja e individit për t'u mbrojtur duhet të jetë në balancë me kujdesin për të mos shkelur vlera dhe liri te tjera themelore demokratike, te tilla si e drejta e informacionit dhe e privatësisë.

Për këto arsye, Autoriteti i Komisionerit ka hartuar këtë udhëzues i cili, parashikon disa rregulla mbi përpunimin e të dhënave personale në ofrimin e shërbimeve cloud computing, duke i ardhur në ndihmë të gjithë subjekteve të të dhënave personale dhe kontrolluesve në këto shërbime.

Ky udhëzues shqyrton mbrojtjen e privatësisë dhe të të dhënave personale në cloud dhe thekson se ky shërbim nuk duhet të çojë në ulje të standardeve për mbrojtjen e të dhënave në krahasim me përpunimin e të dhënave në mënyrë tradicionale.

Udhëzuesi specifikon parimet e përgjithshme, të aplikueshme për kontrolluesit dhe përpunuesit që përpunojnë të dhëna në shërbimet cloud, të tilla si, përcaktimin e qëllimit, fshirjen e të dhënave dhe masat teknike dhe organizative etj. Theks i veçantë është vënë në marrëveshjet kontraktuale që duhet të rregullojnë marrëdhëniet ndërmjet një kontrolluesi dhe një përpunuesi në këtë lidhje. Gjithashtu janë shpjeguar disa nga parimet klasike të të dhënave në aspekt të sigurisë, siç janë disponueshmëria, integriteti dhe konfidencialiteti.

1. ÇFARË ËSHTË CLOUD COMPUTING

Cloud computing është ofrimi i kapaciteteve kompjuterike si shërbim, ku resurset e ndryshme kompjuterike (*hardware)*, programet dhe informacioni, u ofrohen klientëve përmes pajisjeve të ndryshme të teknologjisë së informacionit dhe komunikimit (PC, tablet, *smartphone* etj) në formën e një shërbimi përmes një rrjeti dhe kryesisht aksesohen me nje *browser* [1]përmes internetit.

Llogaritë e email-it (të tilla si Gmail ose Hotmail, etj.) janë shembuj të përditshmërisë së përdorimit të shërbimit cloud, përdoruesit e të cilëve mund të hyjnë në llogarinë e tyre nga çdo vend i botës.

- Ku aplikohen shërbimet "cloud computing" në ditët e sotme? Përdorimi më i zakonshëm ditor janë shembuj për të cilat njerëzit nuk janë në dijeni:

  - Media sociale – FACEBOOK, TWITTER, etj.
  - GOOGLE MAIL & dhe platforma të tjera
  - Telefonat ANDROID & platforma e aplikacioneve të tij:
    - Tregu ANDROID
    - Posta elektronike, kalendari
    - Shërbimet e vendndodhjes gjeografike
  - Telefonat APPLE & platforma e aplikacioneve të tij:
    - Dyqanet APPLE
    - Shërbimet njësoj si për platformën ANDROID
  - Aplikacionet GOOGLE: mbështeten tërësisht në platformën "cloud"

[1] Është një program nëpërmjet të cilit përdoruesit i mundësohet të kërkojë informacion në Internet. (Si psh: Internet Explorer, Mozilla, Opera, etj.)

2. KUSH ËSHTË KLIENTI CLOUD DHE OFRUESI I SHËRBIMIT CLOUD

- Klienti cloud nënkupton kontrolluesin e të dhënave i cili përcakton qëllimin dhe vendos në lidhje me delegimin e plotë ose të pjesshëm të mënyrave të përpunimit të të dhënave nga kompani të jashtme.

- Ofruesi i shërbimit cloud nënkupton përpunuesin i cili ofron mjetet dhe platformën për ofrimin e shërbimeve cloud për llogari të klientit cloud. Kur ofruesi i shërbimit cloud përcakton qëllimin dhe mjetet e përpunimit vepron si kontrollues i përbashkët. Në situata të tilla ofruesi i shërbimit do të mund në parim të konsiderohet si kontrollues i përbashkët në përputhje me përkufizimin e "kontrolluesit" të dhënë në pikën 5, neni 3 i ligjit "Për mbrojtjen e të dhënave personale", i ndryshuar, pasi ai kontribuon në përcaktimin e qëllimeve dhe mjeteve për përpunimin e të dhënave personale.

- Në rastet ku ka kontrollues të përbashkët, përgjegjësitë e secilës palë duhet të jenë të përcaktuara në mënyrë të qartë.

Sa më lart, KDIMDP sugjeron ndarjen e mëposhtme të përgjegjësive:

Rast i prezumuar	Njoftimi pranë KDIMDP	Informimi i subjektit të të dhënave	Detyrimi për ruajtjen e konfidencialitetit dhe sigurisë	Ushtrimi i të drejtave të subjekteve
Ofruesi i shërbimit cloud është kontrollues i përbashkët me klientin cloud	Klienti cloud	Klienti cloud	Ofruesi i shërbimit cloud + Klienti cloud	Klienti cloud me mbështetjen e Ofruesit të shërbimit cloud

3. RREZIQET E PËRDORIMIT TË SHËRBIMEVE CLOUD COMPUTING *(Në kuadër të mbrojtjes së të dhënave personale)*

Informacioni i pamjaftueshëm në lidhje me përpunimin e të dhënave në një shërbim cloud përbën një rrezik për kontrolluesit si dhe subjektet e të dhënave për shkak se ata mund të mos jenë të vetëdijshëm për kërcënimet dhe rreziqet e mundshme dhe në këtë mënyrë nuk mund të marrin masat e përshtatshme.

Disa rreziqe të mundshme mund të lindin për kontrolluesit, nga padijenia se:

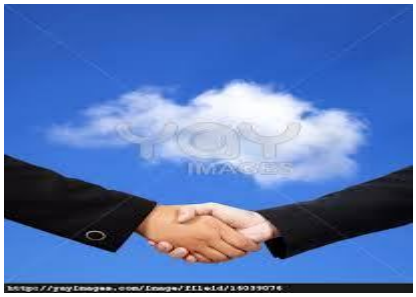
- Po kryhet përpunim zinxhir i të dhënave personale që përfshin përpunues të shumëfishtë dhe nënkontraktorë.

- Të dhënat personale përpunohen në vende të ndryshme gjeografike. Kjo ndikon drejtpërdrejtë në ligjin e aplikueshëm për çdo mosmarrëveshje mbi mbrojtjen e të dhënave që mund të lindin ndërmjet klientit cloud dhe ofruesit të shërbimit cloud.

- Të dhënat personale të transferuara në vende të treta jashtë BE-së. Vendet e treta mund të jenë me nivel jo të mjaftueshëm të mbrojtjes së të dhënave dhe transferimet nuk mund të mbrohen me masa të përshtatshme (p.sh., klauzolat standarde kontraktuale apo rregullat e detyrueshme të korporatave) dhe në këtë mënyrë përpunimi mund të jetë i paligjshëm.

Autoriteti i Komisionerit sugjeron disa nga rregullat që duhen respektuar kur përdoret shërbimit cloud computing, në mënyrë që përpunimi të jetë në përputhje me rregullat për mbrojtjen e të dhënave personale dhe garantimin e sigurisë së të dhënave personale të përpunuara.

4. KONTRATA E SHKRUAR



Klienti cloud dhe ofruesi i shërbimit cloud lidhin një kontratë me shkrim ndërmjet tyre dhe me çdo nën-përpunues në rast delegimi. Kontrata duhet të jetë e qartë në pikat kryesore të përshkruara më poshtë:

- ofruesi i shërbimit cloud dhe çdo nënkontraktor, nëse ka, do të përpunojë të dhënat vetëm siç udhëzohet nga kontrolluesi i të dhënave, pra klienti cloud; dhe
- kontrata të përfshijë siguri të detajuar nga ana e ofruesit të shërbimit cloud, të masave të sigurisë që duhet të merren për të garantuar sigurinë e të dhënave personale kur përpunohen në vende me nivel të pamjaftueshëm.

Kur ofruesi i shërbimit cloud vepron si kontrollues i përbashkët, të drejtat dhe detyrimet e palëve duhet të përcaktohen qartësisht në kontratë, siç është sugjeruar në tabelën e pikës 2 të këtij udhëzuesi.

Kontrata duhet të përcaktojë qartë se ofruesi i shërbimit cloud nuk mund të përdorë të dhënat e kontrolluesit për qëllimet e veta.

5. TRANSPARENCA

Transparenca është thelbësore për një përpunim të drejtë dhe të ligjshëm të të dhënave personale. Transparenca duhet gjithashtu të sigurohet në marrëdhënien ndërmjet klientit cloud, ofruesit të shërbimit cloud dhe nënkontraktorëve (nëse ka). Klienti cloud është në gjendje të vlerësojë vetëm ligjshmërinë e përpunimit të të dhënave personale në cloud, nëse ofruesi informon klientin për të gjitha çështjet relevante. Nëse një kontrollues ka ndërmend të angazhojë një ofrues shërbimi cloud, duhet të kontrollojë me kujdes termat dhe kushtet e ofruesit të shërbimit cloud dhe t'i vlerësojë ato nga këndvështrimi i ruajtjes së privatësisë dhe mbrojtjes së të dhënave personale. **Ndër elementët kryesorë të transparencës janë si më poshtë:**

a) Integriteti

Me anë të integritetit klienti cloud siguron që të dhënat të jenë të sakta, të plota dhe të mos jenë ndryshuar gjatë përpunimit, ruajtjes apo transmetimit, me dashje ose aksidentalisht.

Integriteti përfshin dhe sistemet e teknologjisë së informacionit dhe kërkon që përpunimi i të dhënave personale në këto sisteme të mbetet i pandryshuar. Ndërhyrja

në integritetin e sistemeve të IT në cloud mund të parandalohet apo zbulohet me anë të sistemeve të zbulimit/parandalimit të ndërhyrjeve (IPS/IDS[2]).

b) Konfidencialiteti

Në një mjedis cloud, kodimi ndikon pozitivisht në konfidencialitetin e të dhënave personale. Kodimi i të dhënave personale duhet të kryhet në çdo rast kur të dhënat janë në lëvizje si dhe kur është e mundur, për rastet e tjera. Në disa raste, si IaaS[3] klienti cloud mund të mos mjaftohet me mënyrën e kodimit të ofruar nga ofruesi i shërbimit cloud, por mund të zgjedhë të kodojë vetë të dhënat personale përpara dërgimit të tyre në cloud.

Komunikimi ndërmjet ofruesit të shërbimit cloud dhe klientit cloud, si dhe ndërmjet qendrave të të dhënave duhet të jetë i koduar. Administrimi në distancë i platformës cloud duhet të realizohet vetëm përmes një kanali të sigurt komunikimi. Nëse një klient cloud planifikon, jo vetëm të magazinojë por të përpunojë më tej të dhëna personale në shërbimin cloud (si kërkimi në baza të të dhënave për regjistrimet e kryera), ai duhet të ketë parasysh se kodimi nuk mund të mbahet gjatë përpunimit të të dhënave. Masa të mëtejshme teknike që synojnë sigurimin e konfidencialitetit përfshijnë mekanizmat e autorizimit dhe të autentifikimit të dyfishtë[4]. Dispozita kontraktuale duhet të vendosë detyrime konfidencialiteti mbi punonjësit e klientit cloud, ofruesit e cloud dhe nënkontraktorët.

c) **Disponueshmëria**

Nënkupton ofrimin e aksesit në të dhënat personale në mënyrë të besueshme dhe në kohën e duhur. Ndër rreziqet ndaj disponueshmërisë në cloud janë: humbja aksidentale e lidhjes në rrjet ndërmjet klientit dhe ofruesit të shërbimit, rënie të performancës së shërbimit shkaktuar nga ndërhyrjet e dëmshme (sulmet) të përqendruara, defekte në pajisje, infrastrukturë apo ndërprerje të energjisë elektrike. Kontrolluesit e të dhënave duhet të kenë informacion mbi masat që ka marrë ofruesi i shërbimit cloud për të kufizuar këto rreziqe.

[2] Intrusion Detection and Prevention Systems – janë pajisje sigurie që monitorojnë trafikun e rrjetit për të identifikuar, raportuar ose bllokuar aktivitete që cenojnë sigurinë e rrjetit të brendshëm informatikë.

[3] Infrastructure as a Service – (Infrastruktura si shërbim) kur klienti cloud punon me pajisje hardware/server etj. të vënë në dispozicion nga ofruesi i shërbimit

[4] Autentifikim që bazohet në dy faktorë të pavarur autentifikimi - diçka që vetëm përdoruesi di + diçka që vetëm përdoruesi zotëron.

6. SPECIFIKIMI I QËLLIMIT DHE KUFIZIMI

Klienti përcakton qëllimet e përpunimit përpara mbledhjes së të dhënave nga subjekti i të dhënave dhe e informon këtë të fundit.
Klienti nuk përpunon të dhënat për qëllime të ndryshme nga ai fillestar dhe siguron që të dhënat nuk përpunohen për qëllime të mëtejshme nga ana e ofruesit apo nënkontraktorët.

7. RUAJTJA/FSHIRJA E TË DHËNAVE

Të dhënat personale duhet të mbahen në një formë që lejon identifikimin e subjekteve të të dhënave për jo më shumë se sa është e nevojshme për qëllimin për të cilin të dhënat janë mbledhur ose për të cilin ato përpunohen më tej. Të dhënat personale që nuk janë më të nevojshme duhet të fshihen ose të anonimizohen. Nëse këto të dhëna nuk mund të fshihen për shkak të një detyrimi ligjor që përcakton kohëzgjatjen e ruajtjes (p.sh., legjislacioni tatimor), aksesi në këto të dhëna personale duhet të bllokohet[5].

Parimi i fshirjes së të dhënave zbatohet për të dhëna personale pavarësisht nëse ato mbahen në *hard drives (disqet e ngurta të pajisjeve)* ose në mjete të tjera për *backup* [6]*etj.*
Klienti cloud duhet të sigurohet që ofruesi i shërbimit cloud garanton fshirje të sigurt të të dhënave dhe që në kontratën ndërmjet tyre të parashikohen dispozita të qarta mbi fshirjen e këtyre të dhënave. Kjo dispozitë vlen edhe për kontratën e lidhur ndërmjet ofruesit të shërbimit cloud dhe nënkontraktorët.

8. TË DREJTAT DHE DETYRIMET E KLIENTIT CLOUD

- Klienti cloud duhet të sigurojë paraprakisht një listë të plotë mbi të gjitha vendndodhjet fizike në të cilat magazinohen dhe përpunohen të dhënat personale nga ofruesi i shërbimit cloud ose nënkontraktorët, nëse ka, gjatë gjithë kohëzgjatjes së kontratës, duke përfshirë dhe backup.

[5] Me bllokim kuptojmë ruajtjen e të dhënave personale duke pezulluar përkohësisht çdo veprim tjetër përpunimi.

[6] Kopjimi dhe arkivimi i të dhënave kompjuterike, me qëllim rikthimin në gjendjen origjinale në rast problemesh si humbja apo korruptimi i të dhënave

- **Jashtë kësaj liste, as ofruesi i shërbimit cloud dhe as nënkontraktorët e tij nuk mund të transferojnë të dhënat në vende të tjera nga vende fizike të listuara në kontratë, pavarësisht nëse të dhënat janë të koduara.**

- Klienti cloud ka të drejtë të inspektojë të gjitha vendndodhjet fizike në të cilat përpunohen të dhënat personale tërësisht ose pjesërisht.

- Klienti cloud ka të drejtë të lejojë një palë të tretë të besuar, si një firmë auditimi të njohur, për të monitoruar tërësisht ose pjesërisht përpunimin e të dhënave personale nga ofruesi i shërbimeve cloud dhe nënkontraktorët e tij, nëse ka.

- Klienti cloud duhet të marrë parasysh, nëse është e nevojshme, të ketë akses tek një kopje e të dhënave jashtë kontrollit të ofruesit të shërbimit cloud. Kjo kopje duhet të jetë e aksesueshme dhe e përdorshme në mënyrë të pavarur nga ofruesi i shërbimit cloud ose nënkontraktorët e tij.

- Klienti cloud duhet të përmbushë detyrimet e tij kundrejt subjektit të të dhënave dhe Autoritetit të Komisionerit në rast të shkeljes së të dhënave dhe të marrë masat e duhura. Ai duhet të ketë një marrëveshje të qartë me ofruesin e shërbimit cloud lidhur me njoftimin e menjëhershëm që ofruesi duhet të bëjë pranë klientit cloud dhe/ose Autoritetit të Komisionerit në rast të thyerjes/shkeljes së sigurisë së të dhënave.

- Kontrolluesi duhet të përcaktojë në mënyrë kontraktuale detyrimin e ofruesit të shërbimit cloud për të implementuar proçedura efektive në mënyrë që subjektet e të dhënave të mund të ushtrojnë të drejtat e tyre për akses, korrigjim, fshirje ose bllokim të të dhënave.

9. TË DREJTAT DHE DETYRIMET E OFRUESIT TË SHËRBIMIT CLOUD

- Ofruesi i shërbimit cloud dhe nënkontraktorët nëse ka, duhet të sigurojnë transparencë të plotë për klientin cloud për sa i përket vendndodhjeve në të cilat të dhënat personale përpunohen dhe ruhen.

- Ofruesi i shërbimit cloud duhet të sigurojë transparencë të plotë lidhur me nënkontraktuesit e përdorur për ofrimin e shërbimit dhe se çfarë përpunimi kryejnë ata për llogari të ofruesit të shërbimit cloud.

- Ofruesi i shërbimit cloud duhet të sigurojë transparencë në çështjet kontraktuale dhe të mos ofrojë shërbimin cloud mbi terma dhe kushte standarde që lejojnë ndryshimin e kontratës në mënyrë të njëanshme.

10. AUDITIMI

Duke pasur parasysh mundësinë e grumbullimit të një sasie të madhe të të dhënave personale nga ofruesi i shërbimit cloud, ky i fundit duhet të jetë subjekt i auditeve të palëve të treta përveç auditit të kryer nga vetë klienti cloud. Audituesi duhet të jetë plotësisht i pavarur nga ofruesi i shërbimit cloud dhe duhet t'i kushtojë vëmendje të veçantë aspekteve të sigurisë së përpunimit të të dhënave personale.

Ai duhet të kontrollojë zbatimin e masave për të parandaluar transmetimin e paligjshëm të të dhënave me juridiksione të pamjaftueshme lidhur me mbrojtjen e të dhënave dhe masa për të parandaluar transmetimin e të dhënave në vendndodhje të tjera përtej atyre të rëna dakord shprehimisht me klientin cloud. Audituesi duhet të sigurojë që nuk është e mundur për ofruesin e shërbimit cloud ose nënkontraktorët e tij, shmangia e këtyre masave pa lënë gjurmë.

KOMISIONERI PËR TË DREJTËN E INFORMIMIT DHE MBROJTJEN E TË DHËNAVE PERSONALE

Adresa: "Rr. e Kavajës, Nd. 80, H. 1 - Tiranë

Telefon: +35542237200
E-mail: info@idp.al
Website: www.idp.al

Tiranë 2014