UDHËZIM

Nr. 22, Datë 24.09.2012

PËR
"PËRCAKTIMIN E RREGULLAVE PËR RUAJTJEN E SIGURISË TË TË DHËNAVE PERSONALE TË PËRPUNUARA NGA *SUBJEKTET PËRPUNUESE TË VOGLA*[1]"

Mbështetur në shkronjën "f" të pikës 1 të nenit 31, si dhe në përputhje me detyrimet e përcaktuara në nenin 27, të ligjit nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale" i ndryshuar, Komisioneri për Mbrojtjen e të Dhënave Personale;

UDHËZON:

1. Parashikimin e masave themelore *teknike, organizative edhe në lidhje me personelin*[2], për mbrojtjen e të dhënave personale të përpunuara nga Kontrolluesit e vegjël të të dhënave, ose Përpunuesit, më poshtë referuar subjektet përpunuese të të dhënave personale, dhe rregullat e bashkëpunimit të tyre me Komisionerin.

2. *Subjekte përpunuese të vogla janë kontrolluesit ose përpunuesit të cilët përpunojnë të dhëna personale në mënyrë elektronike ose manuale, duke shfrytëzuar më pak se 6 persona për të kryer përpunimin, qoftë në mënyrë të drejtpërdrejtë ose me anë të përpunuesve.*[3]

3. Kategoritë kryesore të përdoruesve, që detyrohen të ruajnë sigurinë e të dhënave personale, janë:

a) Administratorët e Sistemeve të Teknologjisë së Informacionit, Komunikimit (më tej të quajtur TIK) dhe të Sigurisë së tyre, të cilët zbatojnë këtë detyrim kur subjekti i cili përpunon të dhëna personale ka një sistem TIK të brendshëm dhe/ose të jashtëm të instaluar për këtë qëllim.

b) Operatorët e të dhënave personale (të punësuarit, të kontraktuarit, etj), të cilët përpunojnë të dhëna personale me qëllim, përmbushjen e detyrave të tyre kur punojnë për subjektin përpunues të të dhënave personale.

4. Përveç sa parashikohet në *Udhëzimin nr. 24 , datë 27.12.2012 për "Detyrimet e kontrolluesve përpara se të përpunojnë të dhënat personale"*[4], subjektet përpunuese, duhet të përpunojnë të dhënat personale në përputhje me rregullat e përcaktuara në këtë Udhëzim".

[1] Ndryshuar me Udhëzimin nr. 34, datë 21.1.2013 "Për disa shtesa dhe ndryshime në udhëzimin nr. 22, datë 24.9.2012 për "Përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga kontrolluesit e vegjël".
[2] Ndryshuar me Udhëzimin nr. 34, datë 21.1.2013
[3] Ndryshuar me Udhëzimin nr. 34, datë 21.1.2013
[4] Ndryshuar me Udhëzimin nr. 34, datë 21.1.2013

5. Subjektet përpunuese janë përgjegjës për sigurinë e të dhënave personale duke i mbrojtur ato nga dëmtimet aksidentale apo të paligjshme ose shkatërrimi, humbja aksidentale, ndryshimi, aksesi i paautorizuar dhe vënia në dispozicion personave të paautorizuar, si dhe kundër çdo forme tjetër të paautorizuar të përpunimit. Për këtë qëllim ato duhet të marrin masat e duhura *teknike, organizative edhe në lidhje me personelin*[5], të përshtatshme për mënyrën e përpunimit, dhe duhet të marrin në konsideratë mbi të gjitha:

a) mjetet ekzistuese teknike;

b) nivelin e rrezikut të mundshëm që mund të shkelë sigurinë ose funksionimin e sistemit të të dhënave personale.

6. Subjektet përpunuese duhet të vërtetojnë nivelin dhe përmbajtjen e masave teknike, organizative *edhe në lidhje me personelin* [6]të marra sipas paragrafit 5.

7. Çdo subjekt përpunues mund të autorizojë, me shkrim, një person përgjegjës për mbikëqyrjen e sigurisë së të dhënave personale.

8. Standartet minimale për sigurinë e të dhënave personale duhet të përfshijnë:

a) Analizën e riskut;

1) Analiza e riskut identifikon kërcënimet që prekin pjesë individuale të sistemit të arkivimit, të afta të shkelin sigurinë apo funksionimin e tij. Rezultati i analizës së riskut do të jetë një listë e kërcënimeve që mund të rrezikojnë konfidencialitetin, integritetin dhe disponueshmërinë e të dhënave personale të përpunuara, ndërkohë që ajo do të deklarojë edhe shkallën e riskut të mundshëm, propozimet e masave për eliminimin apo minimizimin e ndikimit të riskut dhe një listë të rreziqeve të mbetura;

2) *Analiza e riskut kryhet në mënyrë periodike dhe dokumentohet në mënyrë të kuptueshme për praktikën e veprimtarisë së subjekteve përpunuese*[7];

b) Sigurinë fizike dhe të ambientit;

1) Sistemet e përpunimit të informacionit, programe ose pajistje TIK ku mbahet një databaze duhet të aksesohen me fjalëkalim. Gjithmonë të bëhet backup-i (një kopje sigurie) i të dhënave në një ambient tjetër të sigurtë.

2) Të lejohet aksesi fizik në pajisjet TIK për përpunimin e të dhënave personale, vetëm për personat e autorizuar dhe të mbahen regjistrime të identitetit të tyre.

[5] Ndryshuar me Udhëzimin nr. 34, datë 21.1.2013
[6] Shtuar me Udhëzimin nr. 34, datë 21.1.2013
[7] Ndryshuar me Udhëzimin nr. 34, datë 21.1.2013

3) Të shkatërrohen përfundimisht të gjitha pajisjet fizike që mbajnë të dhëna personale, kur ato e kanë përmbushur qëllimin për të cilin ishin grumbulluar ose përpunuar dhe në veçanti, letrat e printuara, përfshirë fotokopjet, fotografitë dhe mbartës të tjerë të dhënash, CD ROM, DVD ROM, TAPE, (kaseta regjistruese të Back up), formularë, regjistra fizik.

4) Në rastin e pajisjeve elektronike portative për ruajtjen e të dhënave si dhe pajisjeve memorizuese të tjera, shkatërrimi duhet të bëhet në përmbajtje, në atë mënyrë që të mos jetë i mundur rigjenerimi i informacionit.

5) Të zbatohet politika për *"tavolinat e pastra"* në rastet kur kontraktohen ofrues të shërbimeve të cilët lejohen të hyjnë në ambientet tuaja edhe në mungesën tuaj siç janë, pastrimi i zyrës dhe mirëmbajtja e saj, siguria e ndërtesës, shërbimet teknike, etj.

a) Sigurinë logjike të pajisjeve TIK të përpunimit të të dhënave personale;

1) Nëse keni në zotërim pajisje TIK për përpunimin e të dhënave personale:

a. Të disponohen programe (software) të ligjshëm për përpunimin e të dhënave personale që mundësojnë përditësimet e sigurisë për përdoruesit e ligjshëm.

b. Të instalohen masa sigurie për:

- Garantimin e aksesit individual për ti mundësuar çdo përdoruesi të punojë në llogarinë personale, duke përdorur mjete idendifikimi si *"emër përdoruesi"* dhe *"fjalëkalim";*

- Kufizimin e mundësisë për të lidhur pajisje të jashtme vetëm në varësi të qëllimit që kërkohet si dhe kontrollin e vazhdueshëm të tyre duke bllokuar rrugë të tjera të aksesit.

c. Në rast përdorimi të një shërbimi të jashtëm, të kontraktuar për mirëmbajtjen e pajisjeve TIK të përpunimit të të dhënave personale:

- Punonjësi i palës së kontraktuar, i cili mund të ketë akses në të dhënat personale gjatë zbatimit të detyrave, të trajtohet si përpunuesi juaj;

- Të përfshihet siguria përkatëse e përpunimit të të dhënave në kontratën me këtë palë, duke i garantuar këtij të fundit, akses formal në të dhënat personale apo sistemet të cilat mbartin të dhëna personale.

d. Në rast përdorimi të një shërbimi të jashtëm duke marrë me qira pajisjet TIK për përpunimin e të dhënave personale, atëherë:

- Të përdoren komponentët e sigurisë që këshillohen nga ofruesi i shërbimit;

- Me mbarimin e kontratës së qirasë, të shkatërrohen të dhënat personale nga sistemet dhe pajisjet që do ti kthehen pronarit të pajisjeve TIK, në atë mënyrë që të mos jetë e mundur që informacioni i mëparshëm të rigjenerohet.

2) Aksesi në rrjetet publike;

a. Nëse është e mundur, të kontraktohen ofrues të shërbimit të aksesit në internet që ofrojnë komponentë të sigurisë së rrjetit dhe të instalohen, nëse është e nevojshme, në pajisjet TIK që janë në përdorim.

b. Në rast marrje me qira të pajisjeve për përpunimin e të dhënave personale nga një palë e tretë e specializuar, të kontraktohet shërbimi që ofron komponentë të përditësuar të sigurisë së rrjetit.

c. Në rast përdorimi të lidhjes me internet pa kabëll (*"wireless"),* të mos përdoren pika aksesi të pakoduara dhe të zbatohen standardet e sigurisë për lidhje të tilla.

ç) Sigurinë e personelit;

1) Të punësuarit duhet të informohen mbi rreziqet kryesore ndaj të cilave janë të ekspozuar.

2) Në rastet e punësimeve të reja, të zhvillohen trajnime në varësi të rrezikut të identifikuar dhe për të dhënat personale në lidhje me punësimin të ruhet konfidencialiteti.

3) Të udhëzohet personeli përkatës për ruajtjen e konfidencialitetit të të gjitha mënyrave të verifikimit, idendifikimit që janë vënë në dispozicion, për aksesin në pajisjet TIK të disponueshme, që përdoren për përpunimin e të dhënave personale.

4) Të ndalohet aksesi, menjëherë mbasi punonjësit nuk i kërkohet më të përpunojë të dhënat personale.

9. Për subjektet që përpunojnë të dhëna personale në mënyrë manuale zbatohet dispozitat e parashikuara në pikën 22 të kapitullit III të Udhëzimit nr. 21 datë *24.09.2012* [8]për "Përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga Kontrolluesit e Mëdhenj".

Për zbatimin e këtij udhëzimi ngarkohen kontrolluesit publikë e privatë në territorin e Republikës së Shqipërisë, të përcaktuar në pikën 2 të tij.

Moszbatimi i kërkesave të këtij udhëzimi, përbën shkelje të ligjit për mbrojtjen e të dhënave personale dhe dënohet sipas nenit 39 të ligjit për mbrojtjen e të dhënave personale, i ndryshuar.

Ky udhëzim hyn në fuqi 6 muaj pas botimit në fletore zyrtare.

[8] Ndryshuar me Udhëzimin nr. 34, datë 21.1.2013

KOMISIONERI

FLORA ÇABEJ (POGAÇE)