

Udhëzues për përpunimin e të dhënave personale në administratën publike



**Komisioneri për Mbrojtjen e të Dhënave Personale
Tiranë 2013**

1. Informacion mbi udhëzuesin

Ligji për “Mbrojtjen e të dhënave personale” (këtëj e tutje LMDHP) ka hyrë për herë të parë në fuqi më 10 mars 2008 si dhe ka pësuar ndryshimet e fundit në prill të vitit 2012.

- ❖ **Si objekt ligji parashikon** përcaktimin e rregullave për mbrojtjen dhe përpunimin e ligjshëm të të dhënave personale. Dispozitat e tij gjejnë zbatim si tek kontrolluesit privatë, ashtu edhe tek institucionet e administratës publike.
- ❖ Ky udhëzues u drejtohet të gjithë kontrolluesve të administratës publike. Në të prezantohen parimet e mbrojtjes së të dhënave të cilat duhen respektuar nga ana e administratës publike, ashtu si edhe çështjet të cilat ata duhet të kenë parasysh përpara se të nisë mbledhjen, përpunimin apo transmetimin e të dhënave.



Për të gjitha pyetjet në lidhje me përgjegjësinë e kontrolluesit apo ligjin mbi mbrojtjen e të dhënave personale, në çështje të përgjithshme, ju lutemi t'i drejtoheni personit të ngarkuar për mbrojtjen e të dhënave pranë institucionit tuaj.

2. Kontrolluesi dhe përgjegjësia e tij

Me “kontrollues”, do të kuptojmë autoritetin publik, agjenci apo ndonjë organ tjetër i cili përcakton qëllimin dhe përmbajtjen e dosjeve. Nga këndvështrimi i mbrojtjes së të dhënave, kontrolluesi dhe personi që mbledh apo modifikon të dhënat, mund të jenë dy persona të ndryshëm.

2.1 Përpunimi i të dhënave personale: parime të përgjithshme

Parimet në vazhdim, disa nga të cilat parashikohen nga neni 5 i LMDHP-së, duhet të respektohen në çdo përpunim të dhënash.

- ❖ Të dhënat personale mund të mblidhen vetëm në mënyrë të **ligjshme**.

Do të konsiderohen si të dhëna të mblidhura në mënyra të paligjshme kur ato janë mblidhur me forcë, me mashtrim, apo kërcënim. Duhet nënvizuar se përpunimi i të dhënave duhet të bëhet vetëm nëse parashikohet në ligj.

- ❖ Të dhënat personale duhet të përpunohen konform parimit të **mirëbesimit**;

Kjo nënkupton nga njëra anë, se subjekti i të dhënave ka pasur mundësi ta parashikojë se do t'i mblidhen të dhënat dhe se nga ana tjetër përpunimi i të dhënave do të bëhet me dijeninë e tij.

Do të konsiderohet moszbatim i këtij parimi kur subjekti nuk është vënë në dijeni – apo ka qenë informuar në mënyrë të pasaktë – për qëllimin dhe llojin e përpunimit.

Do të konsiderohen si mashtrim i qëllimshëm çdo përgjim telefonik i paautorizuar, mbledhja e të dhënave pa dijeninë e subjektit me anë të manipulimit të programeve, apo mbledhja sekrete e të dhënave, që nuk është parashikuar qartësisht nga një ligj.

- ❖ Të dhënat personale nuk mund të përpunohen përveçse për **qëllimin përfundimtar** që është përcaktuar përpara mbledhjes, që parashikohet nga ligji apo që rrjedh prej rrethanave.

Çdo person që disponon një dosje, duhet të sigurohet se të dhënat që ndodhen në dosje janë **të sakta**. Me fjalë të tjera, duhet nga njëra anë që të dhënat të jenë të përditësuara dhe ana tjetër, që ato të mund të korrigjohen nëse janë të pasakta.

- ❖ Të dhënat duhet të përpunohen në mënyrë **proporcionale**.

Çdo përpunim të dhënash personale përbën një cënim ndaj personalitetit dhe prandaj duhet pasur kujdes të kufizohet ky cënim sa më shumë të jetë e mundur.

Për këtë arsye, kontrolluesi nuk ka të drejtë të përpunojë veçse të dhënat të cilat i duhen patjetër dhe që janë të nevojshme për kryerjen e detyrës së tij. Ju duhet të fshini pra, ose të arkivoni të dhënat në çastin kur ju nuk iu nevojiten.

Mbledhja e të dhënave personale dhe në veçanti qëllimi i përpunimit të tyre, duhet t'i informohet subjektit të të dhënave.

- ❖ Kërkesa për të informuar mbi përpunimin, konkretizon parimin e mirëbesimit dhe synon kështu të bëjë përpunimin më transparent.

Ky parim nënkupton se subjekti i të dhënave duhet të jetë në dijeni, në kushte normale, se të dhënat që i përkasin janë mbledhur ose do të mblidhen.

Subjekti duhet gjithashtu të dijë qëllimin e përpunimit të të dhënave apo të mund të konstatojë se qëllimi i është bërë me dije gjatë mbledhjes apo ka dalë në pah nga rrethanat.

2.1.1 Baza ligjore

Administrata publike nuk mund të përpunojë të dhënat përveçse kur bazohet në një parashikim ligjor.

Sa më i lartë të jetë rreziku i cënimit të të dhënave aq më të forta do të jenë edhe kriteret për përpunimin e tyre.

Për këto arsye, nëse duam të përpunojmë të dhëna sensitive, rregulli i përgjithshëm është të ketë bazë ligjore të veçantë.

Megjithatë, neni 7 i LMDHP-së, parashikon rastet kur është e mundur të përpunohen të dhëna sensitive pa pasur bazë ligjore të veçantë, të cilat janë:

- ❖ Kur subjekti i të dhënave ka dhënë pëlqimin;
- ❖ Kur duhet patjetër, për përmbushjen e një detyrimi të përcaktuar qartësisht nga një ligj i veçantë;
- ❖ Kur është në interesin jetik të subjektit të të dhënave ose të një personi tjetër;
- ❖ Kur autorizohet nga autoriteti përgjegjës për një interes të rëndësishëm publik, nën masa të përshtatshme mbrojtëse;
- ❖ Kur të dhënat, janë bërë hapazi publike nga subjekti i të dhënave;
- ❖ Kur të dhënat përpunohen për qëllime historike, shkencore ose statistikore, nën masa të përshtatshme mbrojtëse;
- ❖ Kur të dhënat kërkohen për qëllime të mjekësisë parandaluese, diagnostikimit mjekësor, etj.

2.2 Mbledhja e të dhënave personale

Përpunimi i ligjshëm i të dhënave personale nënkupton gjithashtu mbledhjen bazuar në ligj të këtyre të dhënave. Kështu, nëse një organ i administratës publike mbledh sistematikisht të dhëna, ai është i detyruar t'u komunikojë subjekteve të përfshirë elementet në vazhdim:

- ❖ Qëllimin e përpunimit,
- ❖ Bazën ligjore të përpunimit;
- ❖ Kategoritë e marrësve të të dhënave;
- ❖ Kategoritë e të dhënave;
- ❖ Marrësit e të dhënave.

Mbledhja e të dhënave sensitive duhet të kryhet me dijeninë e subjektit të të dhënave, përveçse nëse një ligj e përcakton ndryshe.

Çdo mbledhje të dhënash që do të kryhet sipas një procedure tjetër, do të bjerë ndesh patjetër me parimet e përgjithshme të mbrojtjes së të dhënave.

Ju nuk mund të mblidhni të dhëna përveçse nëse keni patjetër nevojë për përmbushjen e detyrave tuaja ligjore. Për rrjedhojë, jeni të detyruar t'i shkatërroni kur të mos keni më nevojë, përveçse nëse ka një afat kohor për arkivimin e tyre të përcaktuar në ndonjë akt ligjor.

Kur mblidhni të dhëna, duhet të informoni subjektet për këtë veprim, nëse nuk del në pah nga rrethanat.



Ne ju këshillojmë të verifikoni saktësinë e të dhënave.

Kështu do të shmangni kërkesat e panevojshme për informacion.

2.3 Transferimi i të dhënave jashtë vendit

Transferimi i të dhënave personale jashtë vendit, mund të çenojë personalitetin e subjektit të të dhënave, edhe në qoftë se përpunimi i këtyre të dhënave nuk paraqet asnjë problem në Shqipëri.

Për këtë arsye, transferimi i të dhënave drejt vendeve që nuk kanë nivel mbrojtjeje të përshtatshëm duhet të kryhet vetëm bazuar në kushtet e parashikuara nga nenet 8 dhe 9 të LMDHP-së.

Në parim, Shtetet që kanë ratifikuar Konventës Nr. 108 "Për mbrojtjen e individëve në lidhje me përpunimin automatik të të dhënave personale" si dhe protokollin përkatës shtesë, ofrojnë nivel mbrojtjeje të përshtatshëm.

I tillë është rasti për vendet e BE-së.

- ❖ Për të lehtësuar vlerësimin e situatës në rast transferimi të të dhënave jashtë vendit (dhe me qëllim informimin e subjekteve të përfshirë), autoriteti i Komisionerit për mbrojtjen e të dhënave personale (këtej e tutje KMDP-ja) ka përcaktuar një listë shtetesh që kanë legjislacion që siguron nivel mbrojtjeje të përshtatshëm.

Kjo listë mund të gjendet në Vendimin Nr. 3, datë 20.11.2012 "Për përcaktimin e shteteve, me nivel të mjaftueshëm të mbrojtjes së të dhënave personale" e cila është e publikuar edhe në faqen zyrtare të KMDP-së, www.kmdp.al.

Administrata publike është e detyruar të respektojë kushtet e përpunimit të të dhënave personale që legjislacioni mbi mbrojtjen e të dhënave parashikon për transferimin e të dhënave.

2.4 Kërkesat dhe procedura

Çdo person që provon se ka interes legjitim mund t'i kërkojë organit kompetent,

- ❖ të konstatojë karakterin e paligjshëm të një përpunimi të dhënash;
- ❖ të ndalojë përpunimin e paligjshëm të të dhënave;
- ❖ të kërkojë korigjimin, bllokimin ose fshirjen e të dhënave; apo
- ❖ ta informojë mbi të dhënat të cilat e përfshijnë.

Sipas praktikës administrative aktuale, jo vetëm subjektet e përfshira mund të paraqesin pretendime të tilla, por gjithashtu edhe palë të treta, në rrethana të caktuara në përputhje me Kodin e Procedurës Civile.

Pas ankimit administrativ, subjekti i të dhënave mund t'i drejtohet Komisionerit për Mbrojtjen e të Dhënave për të kërkuar zbatimin e të drejtave të tij.

2.4.1 Detyrimi për të dhënë informacion

Çdo person të cilit ju i përpunoni të dhënat, ka të drejtë të kërkojë informacione **pa pagesë** mbi të dhënat në fjalë, për të kërkuar, nëse paraqitet nevoja, që ato të korigjohen apo të fshihen. (kreu IV i LMDHP)

Të vetmet kufizime në këtë të drejtë aksesi, janë ato të parashikuara nga neni 12 i LMDHP-së: Mund të ketë kufizim nëse çënohen:

- ❖ interesat e sigurisë kombëtare,
- ❖ politika e jashtme,
- ❖ interesat ekonomikë dhe financiarë të shtetit,
- ❖ parandalimi dhe ndjekja e veprave penale.

Nëse kufizoni të drejtën e aksesit, jeni të detyruar të informoni **me shkrim subjektin kërkues** brenda 30 ditëve dhe të argumentoni vendimin.

E drejta e aksesit është instrumenti juridik më i rëndësishëm i ligjit mbi mbrojtjen e të dhënave personale. Ai përbën mjetin e vetëm për subjektin e përfshirë, që të kërkojë të drejtat e tij në fushën e mbrojtjes së të dhënave. Duhet pasur kujdes pra, që kjo e drejtë, të mos kufizohet, përveçse kur është absolutisht e nevojshme.



Sigurohuni që parimi i transparencës së aktiviteteve administrative, mbi të gjitha çështjet që lidhen me ushtrimin e të drejtës së aksesit, të respektohen.

2.5 Siguria e të dhënave

Ndërsa mbrojtja e të dhënave personale ka për qëllim **të mbrojë personalitetin**, siguria e të dhënave synon **të mbrojë informacionin**, thënë ndryshe, të garantojë:

- ❖ Konfidencialitetin;
- ❖ Disponueshmërinë; dhe
- ❖ Integritetin.

Organet e administratës publike mbajnë evidenca dhe regjistra të ndryshëm që kanë të bëjnë pjesërisht ose plotësisht me të dhënat e qytetarëve (p.sh., evidencat e të lindurve, të martuarve, të vdekurve, dhe evidencat për detyrimet tatimore, etj). Megjithatë, edhe organet e tjera shtetërore, gjykatat dhe personat juridikë të autorizuar me ligj, mbajnë evidenca të të dhënave të shumëllojshme në të cilat përfshihen të dhënat personale të qytetarëve (Regjistri Kombëtar i Gjendjes Civile, etj.) Duke u nisur nga kjo, mbrojtja e të dhënave personale e qytetarëve, si e drejtë kushtetuese e garantuar, shfaqet si një çështje e rëndësishme në lidhje me veprimtarinë e përditshme të një numri të madh organesh të sektorit publik.

Nëpunësit e administratës publike edhe pas largimit nga detyra nuk duhet ta përdorin informacionin konfidencial, të marrë gjatë kryerjes së detyrës, për interes personal.

Sa i përket sigurisë së të dhënave, ajo përfshin të gjitha masat që duhen marrë nga ana e kontrolluesit, për të përmbushur kërkesat e parashikuara nga ligji mbi mbrojtjen e të dhënave.

Çdo institucion i administratës publike ndër të tjera mban dhe dosjet e personelit për nëpunësit e tij.

Dosjet përmbajnë të dhëna personale dhe profesionale të nëpunësve civilë dhe për këtë arsye do të përdoren në përputhje me LMDHP.

Në këtë mënyrë, ato duhet të jenë të disponueshme vetëm për:

- ❖ Nëpunësin në lidhje me të dhënat e tij;
- ❖ Komisionin e Shërbimit Civil;
- ❖ Gjykatat si dhe çdo institucion tjetër i parashikuar me ligj.

Neni 27 i LMDHP-së, parashikon se të dhënat personale duhet të mbrohen nga çdo përpunim i paautorizuar, me masa organizative dhe teknike të përshtatshme. Këto masa përfshijnë midis të tjerash, kontrollin e aksesit tek të dhënat, transferimin, komunikimin, ruajtjen dhe përdorimin e të dhënave personale.

Për të pasur informacion më të plotë mbi çështjen e sigurisë, shikoni Udhëzimet e miratuara nga Autoriteti i Komisionerit në lidhje me masat teknike dhe organizative të mbrojtjes së të dhënave.

Më konkretisht:

- ❖ Udhëzimi Nr. 21, datë 24.09.2012 për “Përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga kontrolluesit e mëdhenj”, i ndryshuar;
- ❖ Udhëzimin Nr. 22, datë 24.09.2012 për "Përcaktimin e rregullave për ruajtjen e sigurisë të të dhënave personale të përpunuara nga kontrolluesit e vegjël", i ndryshuar.

3. Disa udhëzime të vlefshme për mbrojtjen e të dhënave

Për të lehtësuar punën tuaj të përditshme duhet fillimisht të përpiloni një listë të të gjitha dosjeve, struktura e të cilave mundëson kërkimin e të dhënave sipas personit dhe do t’ju lejojë të përcaktoni se kush i mbledh të dhënat, cilat të dhëna mblidhen dhe për çfarë qëllimi.

Kjo listë do t’ju ndihmojë të zbatoni në mënyrë më efektive masat e nevojshme për një përpunim të drejtë dhe të ligjshëm të të dhënave.

- ❖ Në shumicën e institucioneve shtetërore, tashmë është caktuar një Person i Ngarkuar për mbrojtjen e të dhënave personale i cili do të koordinojë punën me Autoritetin e Komisionerit.

Eksperiencat në legjislacionin e Bashkimit Evropian, tregojnë se një person i tillë është jashtëzakonisht i nevojshëm, veçanërisht për të gjitha detyrat e këshillimit, planifikimit dhe koordinimit.

Bëhet fjalë shpesh për të vetmin mjet për përmbushjen e të gjitha kërkesave në fushën e mbrojtjes së të dhënave personale. Mos ngurroni pra, t'i drejtoheni Personit të Ngarkuar për mbrojtjen e të dhënave nëse hasni probleme sado të vogla në këtë fushë si dhe vetë Autoritetit të Komisionerit i cili do të jetë i angazhuar në çdo kohë për t'ju ardhur në ndihmë.

Mendojeni: një përpunim të dhënash që nuk respekton parimet e mbrojtjes së të dhënave personale, mund të dëmtojë imazhin tuaj ashtu si edhe të institucionit tuaj!



KOMISIONERI PËR MBROJTJEN E TË DHËNAVE PERSONALE

Adresa: Rr. “Abdi Toptani”, Godina e Ish/M.T dhe Telekomunikacioneve, Kati i II-të, Tiranë.

Telefoni: +35542237200

E-maili: info@kmdp.al

Website: www.kmdp.al

Tiranë 2013

Ky udhëzues u përgatit nga Drejtoria e Çështjeve Proçedurale Ligjore dhe Marrëdhënieve me Jashtë: **Anola Shala**, Drejtoresh; **Elda Faruku**, Specialiste