Agjencia Shtetërore për Mbrojtjen e të Dhënave Personale
Državna Agencija za Zaštitu Ličnih Podataka
National Agency for Protection of Personal Data

Manual

"Mbi udhëzimet për zbatimin e LMDHP-së në sferën e sigurisë së të dhënave personale"

Prill, 2016

Përmbajtja

1 Siguria e të dhënave personale – Konceptet themelore, obligimet ligjore dhe rekomandimet

Një nga obligimet themelore të çdo kontrolluesi dhe përpunuesi (të referuar më vonë si Përpunues apo Kontrollues i përpunimit të të dhënave) është ofrimi i sigurisë së të dhënave, d.m.th zbatimi i masave të duhura teknike dhe organizative me qëllim të mbrojtjes së të dhënave personale nga shkatërrimi aksidental apo i paligjshëm apo humbja aksidentale, ndryshimi, shpalosja apo qasja e paautorizuar. Gjithashtu mbulon edhe përpunimin që përfshin transmetimin e të dhënave përmes rrjeteve lokale dhe publike. Siguria në aspektin ligjor gjithashtu mbulon edhe mbrojtjen ndaj të gjitha formave tjera të paligjshme të përpunimit. Masat e zbatuara të sigurisë duhet të jenë adekuate për dobësitë dhe rreziqet e identifikuara dhe për kategoritë e të dhënave - masa të veçanta të sigurisë që duhet të zbatohen për përpunimin e "të dhënave të ndjeshme." Kërkesa për mjaftueshmërinë kërkon mjete për zbutjen e rreziqeve të cilat janë në gjendje të ofrojnë nivelin e sigurisë të paraparë me ligj dhe ky ligj nuk e bën të detyrueshëm obligimin për miratimin e masave "kozmike" të sigurisë që do të ishin shkatërruese për Përpunuesin apo Kontrolluesin e përpunimit të të dhënave (kontrolluesi ose përpunuesi).

Ofrimi i sigurisë së të dhënave nuk është një detyrë e vetme që ndodh vetëm një herë, por është obligim i vazhdueshëm i të qenit një "proces i biznesit," kështu që kërkon burime të duhura njerëzore dhe kapitale në bazë të përhershme që duhet të garantohen. Obligimi për të siguruar të dhënat është i caktuar për çdo Përpunues dhe Kontrollues të përpunimit të të dhënave, pavarësisht rëndësisë së saj, formës së pronësisë dhe/ose madhësisë. Gjithashtu mbulon të gjitha llojet e përpunimit manual.

Masat e sigurisë që janë të vendosura duhet të pasqyrojnë kërcënimet dhe dobësitë reale të mjedisit të caktuar ku përpunohen të dhënat.

Për organet private dhe publike që përpunojnë të dhëna me rrezik të ulët, terminologjia përshkruese duhet të thjeshtësohet në mënyrë përkatëse në mënyrë që të jetë sa më afër që të jetë e mundur me gjuhën e përdorur për praktikat e përbashkëta të biznesit të organeve të tilla private dhe publike, në sektorin e veçantë të ekonomisë.

Termet kanë kuptimin si në vijim:

1. **Konfidencialiteti** – sigurimi se informacioni nuk është vënë në dispozicion apo nuk iu është shpalosur personave të paautorizuar, organeve private dhe publike apo proceseve.
2. **Integriteti** – sigurimi se të dhënat nuk janë ndryshuar apo shkatërruar në mënyrë të paautorizuar, duke ruajtur në këtë mënyrë saktësinë dhe plotësinë e të dhënave dhe metodat e përpunimit.
3. **Disponueshmëria** – sigurimi që të jenë në dispozicion dhe ekziston mundësia që të përdoren sipas kërkesës, brenda kohës dhe vendit specifik, në dispozicion për personat e autorizuar dhe për sistemet e përpunimit kur kërkohen.
4. **Llogaridhënia** e sistemeve të TIK-ut që aplikohen për përpunimin e të dhënave dhe personelit që operon me to, duke garantuar kështu që secili aktivitet i tyre i zbatuar për të dhënat është i gjurmueshëm dhe i audituesheëm.
5. **Mos-refuzimi** – asnjë mundësi që t'i mohohet përfshirja e dikujt (stafit apo sistemeve të përpunimit të të dhënave), pjesërisht apo në tërësi në përpunimin e të dhënave.

Organet private dhe publike që kryejnë përpunimin janë përgjegjëse për sigurinë e të dhënave personale duke i mbrojtur nga dëmtimi apo shkatërrimi aksidental apo i paligjshëm, humbjet aksidentale, qasja e paautorizuar dhe vënia në dispozicion, si dhe nga çfarëdo forme tjetër e paautorizuar e përpunimit. Për këtë qëllim, ata duhet të vendosin masa adekuate teknike dhe organizative ndaj kërcënimeve dhe dobësive ndaj të cilave ekspozohet ky përpunim i veçantë. Ata duhet të marrin parasysh të gjitha dobësitë dhe kërcënimet që mund të materializohen në rreziqe, duke i trajtuar ato në një mënyre logjike (adekuate) me prioritet.

Kategoritë kryesore të personave përgjegjës për detyrën e sigurimit të përpunimit të të dhënave personale janë:

- **Administratoret** e sistemeve të Teknologjisë së Informacionit dhe Komunikimit (këtu e tutje TIK) dhe sigurisë së tyre, të cilët janë subjekt i këtij obligimi kur Përpunuesi apo Kontrolluesi i cili përpunon të dhënat personale ka një sistem të TIK-ut të brendshëm dhe/ose të jashtëm të krijuar për qëllime të tilla.
- **Operatorët** (punonjësit, kontraktuesit, etj) e të dhënave personale që përpunojnë të dhënat personale duke përdorur mjetet e TIK-ut me qëllim të përmbushjes së detyrave të tyre përderisa punojnë për Përpunuesit apo Kontrolluesit e përpunimit të të dhënave personale.
- **Të gjithë personat tjerë** të caktuar nga Përpunuesi apo Kontrolluesi i përpunimit të të dhënave për përpunimin manual të të dhënave.

Mbani në mend:

- *"**Operatorët**" nuk duhet të ngatërrohen me "përpunuesit": Operatori është personi fizik që kryen detyrën e përpunimit të të dhënave për një kontrollues apo përpunues Në rast të një kompanie të vogël me 1-person i cili është përpunues, përpunuesi i tillë mund në të njëjtën kohë të veprojë edhe si operator.*
- *Në aspektin e sigurisë së përpunimit të të dhënave personale, organet publike dhe private janë të obliguara t'i ndjekin jo vetëm ligjet e përgjithshme për mbrojtjen e të dhënave personale të nxjerra nga parlamenti, por edhe aktet nënligjore sekondare të nxjerra nga qeveria si dhe Udhëzimet Administrative dhe udhëzimet e veçanta të ASHMDHP-së. Gjithashtu, ata janë të detyruar t'i ndjekin të gjitha ligjet, aktet nënligjore dhe kodet e praktikës së mirë që janë specifike për sektorin, të cilat janë të prezantuara si mjete për vetë-rregullim.*

2 Trajtimi i rreziqeve të mëdha për përpunimin e të dhënave personale

Një pikënisje e mirë është një rishikim themelor logjik i dobësive dhe kërcënimeve ndaj të cilave është subjekt përpunimi juaj i të dhënave. Një analizë dhe vlerësim i tillë kërkon përgjigjen e pyetjeve në vijim:

- Cilat janë kërcënimet dhe dobësitë e mëdha në mesin e të gjitha rrjedhave të përpunimit të informacionit të cilat gjithashtu përfshijnë të dhëna personale?
- Cilat nga to kanë më shumë gjasa të materializohen në format e rreziqeve të vërteta?
- Cilat nga këto rreziqe kanë më shumë gjasa t'i nënshtrohen shkeljes të të dhënave që shpijnë në dëmtim apo humbje?
- Cilat nga to kërkojnë monitorim të rregullt në mënyrë që të lehtësohet në nivelin e pranueshëm?
- Cilat mjete dhe masa për parandalim dhe zbutje mund të propozohen duke pasur parasysh burimet e kufizuara që mund t'i përkushtohen sigurisë?
- Si duhet të organizohen këto masa në aspektin e ngarkimit të përgjegjësive tek akterët e ndryshëm dhe ZMDH?

***Vërejte e rëndësishme**: dobësitë dhe rreziqet nuk duhet të perceptohen si të ndërlidhura dhe që rezultojnë nga vetëm TIK, ato gjithashtu shfaqen gjatë rrjedhës së përpunimit manual dhe faktori më i dobët është gjithmonë qenia njerëzore - në veçanti përdoruesi i mjeteve të TIK-ut. Kjo është veçanërisht e rëndësishme nga perspektiva e mbrojtjes së të dhënave personale, ku gabimi njerëzor mund të rezultojë lehtësisht në një shpalosje të paligjshme dhe serioze të të dhënave personale (shkelja e të dhënave). Për këtë arsye, duhet të përfundohet një analizë dhe vlerësim i tillë në mënyrën e përshkruar më poshtë.*

2.1 Kontrolli i pajtueshmërisë ligjore

Aktiviteti i parë është gjithmonë lista e akteve ligjore në lidhje me përpunimin e të dhënave personale, ndaj së cilës i nënshtrohet përpunimi i veçantë. Kjo zakonisht rezulton me një listë sikurse:

- Aktet ligjore që rregullojnë rregullat e përgjithshme (ligjin e përgjithshëm për mbrojtjen e të dhënave) të përpunimit të të dhënave personale, duke përfshirë aktet nënligjore që mbulojnë fushat specifike - sidomos çështjet e sigurisë.
- Ligjet specifike sektoriale që gjithashtu rregullojnë mbrojtjen e të dhënave personale, edhe në qoftë se ata nuk referohen drejtpërdrejtë të dhënave personale dhe mbrojtjen e tyre.

Kjo është shumë e rëndësishme, pasi që kompetenca në konfidencialitetet specifike sektoriale dhe regjimet e ndërlidhura të sigurisë janë absolutisht vendimtare për interpretimin e duhur të rregullave të përgjithshme të ligjit për mbrojtjen e të dhënave personale në rrethana të veçanta. Këto ligje specifike sektoriale në lidhje me të dhënat personale përdoren për të rregulluar aspektet e tilla si shembull.:

- Rregullat detyruese ligjore mbi shpërndarjen e të dhënave
- Periudhat e ruajtjes së të dhënave
- Masa e pëlqimit të pranueshëm, kërkesat shtesë për ta bërë atë ligjërisht detyruese, veçanërisht në formë elektronike
- Masat shtesë teknike dhe organizative të sigurisë
- Transferimet e të dhënave, shpalosjet e detyrueshme tek organet tjera private dhe publike (p.sh. shkëmbimi i të dhënave ndërmjet institucioneve publike).
- Kërkesat shtesë të VNP (Vlerësimi i Ndikimit të Privatësisë), p.sh. ato që rezultojnë nga angazhimi në forma të ndryshme të përpunimit elektronik, masa dhe format e kontraktimit, etj.

Mbani në mend! - *Edhe pse duken të mos jenë të lidhura drejtpërdrejt me sigurinë e të dhënave, ato gjithmonë rezultojnë me disa obligime të ndërlidhura me sigurinë - çdo obligim ligjor përkthehet në një regjim përkatës të sigurisë që kërkohet në mënyrë që të arrihet*

pajtueshmëria e kërkuar ligjore përmes disa mjeteve dhe masave teknike. Në një formë të avancuar, ajo rezulton në drejtime të caktuara që vjen nga një VNP formale.

2.2 Pajtueshmëria e sigurisë e ndërlidhur me TIK

Aktiviteti i ardhshëm është një vlerësim i përgjithshëm i asaj se si rregullohet përpunimi i TIK në aspektin e gjenerimit të rreziqeve për mbrojtjen e të dhënave personale.

Në përgjithësi duhet të shqyrtohen dy aspekte:

- Përpunimi i TIK duke përdorur burimet vetanake, kur kompetenca e përpunimit të TIK mbetet në vend,
- Përpunimi i deleguar i TIK. Ndërlidhet me situata si mbështetja në palët e treta të jashtme profesionale për realizimin e përpunimit të të dhënave, kur palët e treta të tilla ofrojnë harduer, softuer dhe/ose përkrahje (forma dhe shkallë të ndryshme të delegimit të tillë mund të organizohen këtu, jo gjithë prej tyre janë subjekt i ligjit për mbrojtjen e të dhënave - aftësia e palës së tretë për qasje në të dhënat personale është vendimtare).

3 Obligimet e përbashkëta mbi sigurinë e të dhënave për çdo Kontrollues dhe Përpunues ligjor që përpunon të dhëna personale

Grupi themelor i obligimeve të sigurisë së të dhënave përcaktohet me Ligjin Nr. 03/L-172 për mbrojtjen e të dhënave personale. Këto obligime janë cituar më poshtë (sipas rendit të paraqitur në Akt) dhe shoqërohen me shënime shpjeguese – të kufizuara në çështjet e sigurisë.

Mbrojtja e të dhënave personale të ndjeshme (Neni 7)

1. Të dhënat personale të ndjeshme duhet të mbrohen në mënyrë të veçantë dhe të klasifikohen me qëllim të parandalimit të qasjes dhe përdorimit të paautorizuar, me përjashtim të rasteve nga nën-paragrafi 1.5, paragrafit 1 të nenit 6 të këtij ligji.
2. Kur të dhënat personale të ndjeshme transferohen përmes rrjeteve të telekomunikimit konsiderohen si të mbrojtura në mënyrë të përshtatshme, nëse ato janë të koduara për të siguruar mos-lejueshmërinë dhe mos-njohjen e tyre.

Kjo përcakton masa shtesë mbrojtëse për të dhënat e ndjeshme. Në aspektin e enkriptimit, minimumi është që të bëhet enkriptimi i trafikut të të dhënave në rrjete. Kjo mund të interpretohet edhe si enkriptim i përmbajtjes për kohë më të gjatë se sa vetë transmetimi.

Siguria e përpunimit të të dhënave (Neni 14)

1. Sigurimi i të dhënave personale përfshinë procedurat dhe masat e duhura organizative, teknike dhe logjiko-teknike për mbrojtjen e tyre dhe parandalimin e çfarëdo shkatërrimi të paqëllimshëm ose të qëllimshëm të paautorizuar, zbulimin, ndryshimin, qasjen ose përdorimin e të dhënave apo humbjen e papritur ose të qëllimshme të tyre si:
   1.1. duke i mbrojtur lokalet, pajisjet dhe sistemet aplikative (softuerët), përfshirë edhe kontrollin e qasjes;
   1.2. duke i mbrojtur programet aplikative (softuerike) që përdoren për

përpunimin e të dhënave;

1.3. duke parandaluar çfarëdo qasje të paautorizuar në ose leximin e të dhënave personale gjatë ruajtjes dhe transmetimit të tyre, përfshirë transmetimin nëpërmjet mjeteve të telekomunikimit dhe rrjeteve;

1.4. duke siguruar metodat efikase për bllokimin, shkatërrimin, fshirjen ose anonimizimin e të dhënave personale;

1.5. duke mundësuar përcaktimin pasues se kur janë futur të dhënat personale në sistemin e dosjeve, kur janë qasur, ndryshuar, zbuluar, shkatërruar, përdorur ose kur janë përpunuar ndryshe, dhe kush e ka bërë atë, për kohën sa janë ruajtur ato.

2. Nëse të dhënat personale janë përpunuar me anë të rrjeteve të telekomunikimit duhet të sigurohet që përpunimi të kryhet brenda kufijve të paraparë me ligj. Gjithashtu pajisjet e prekshme (hardueri), programi sistemor (softueri) dhe aplikacionet programore (softuerike) duhet të sigurojnë një nivel të përshtatshëm të mbrojtjes së të dhënave.
3. Procedurat dhe masat për të mbrojtur të dhënat personale duhet të jenë të përshtatshme dhe të mbahen të përditësuara, duke pasur parasysh natyrën e të dhënave personale që duhet mbrojtur dhe rrezikun që paraqitet gjatë përpunimit të të dhënave të tilla.
4. Zyrtarët, të punësuarit dhe personat tjerë që kryejnë punë lidhur me përpunimin e të dhënave përfshirë kontrolluesin e të dhënave janë të obliguar, që gjatë dhe pas kryerjes së punëve të kontraktuara, të mbrojnë fshehtësinë e të dhënave personale me të cilat ata njihen.

Mbani në mend:

- *Ligji për mbrojtjen e të dhënave zbaton QASJEN E BAZUAR NË RREZIK për sigurinë e të dhënave.*
- *Pasi që qëllimi kryesor i këtij ligji është mbrojtja e të drejtave të subjektit të të dhënave, Vlerësimi i Ndikimit mbi Privatësinë (VNP), siç shihet nga perspektiva e subjekteve të të dhënave (të dhënat e të cilëve përpunohen), duhet gjithashtu të përfshihet në një analizë dhe vlerësim të tillë të rreziqeve.*

- *Për këtë arsye, para përpunimit të të dhënave personale, Kontrolluesi apo Përpunuesi duhet të kryej një vlerësim të një ndikimi të operacioneve të parapara të përpunimit për mbrojtjen e të dhënave personale ku këto operacione të përpunimit mund të paraqesin rreziqe të veçanta për të drejtat dhe liritë e subjekteve të të dhënave për shkak të natyrës, fushëveprimit apo qëllimeve të tyre.*
- *Një analizë e tillë duhet të bëhet para se të shkohet në diskutime teknike mbi atë se si të bëhet një përpunim i tillë i sigurt, pasi që ndihmon në mënyrë të konsiderueshme në identifikimin e atyre pjesëve të përpunimit të të dhënave ku siguria është më e rëndësishmja nga pikëpamja e mbrojtjes së të dhënave.*
- *Rezultati i kësaj analize nuk është identik me vlerësimin e rreziqeve nga Kontrolluesi dhe Përpunuesi si një sipërmarrës, pasi që vlerësimi i tyre i rreziqeve është për nga natyra i përqendruar në mbrojtjen e aseteve të vlefshme të informacionit.*
- *Roli i ZMDH-së është mbikëqyrja e vlerësimit të tillë dhe realizimi i tij.*

Obligimi për të siguruar të dhënat personale (Neni 16)

1. Kontrolluesit e të dhënave dhe përpunuesit e të dhënave duhet të kujdesen në çfarëdo kohe se të dhënat personale mbrohen në mënyrën e përcaktuar në Nenin 14 të këtij Ligji.
2. Kontrolluesit e të dhënave dhe përpunuesit e të dhënave duhet të përshkruajnë në aktet e tyre të brendshme procedurat dhe masat e krijuara për sigurinë e të dhënave personale dhe duhet të emërojnë me shkrim personat kompetent të cilët janë përgjegjës për sistemet e dosjeve dhe ata të cilët, për shkak të natyrës së punës së tyre, duhet të përpunojnë të dhënat personale. 12

Komenti shpjegues:

Këto dy nene obligojnë Kontrolluesin dhe Përpunuesin të ndërmarrin masat e duhura organizative dhe teknike në mënyrë që të mbrojnë të dhënat personale nga shkatërrimi i paligjshëm apo aksidental, humbja aksidentale, nga qasja apo shpalosja tek personat e paautorizuar, veçanërisht kur përpunimi i të dhënave zhvillohet në një rrjet, si dhe nga çfarëdo forme e paligjshme e përpunimit.

Ato specifikojnë grupin minimal të detyrueshëm të masave të sigurisë që duhet të futen në mënyrë të dokumentuar. Ato obligojnë një ndarje të qartë të përgjegjësive për ruajtjen e sigurisë së informacionit - pa specifikuar saktësisht se çfarë masa organizative dhe teknike të sigurisë duhet të vendosen. Thekson rolin e autorizimit të duhur si një parakusht për të lejuar përpunimin e të dhënave personale dhe obligon organet private dhe publike për përpunimin e të dhënave që të dokumentojnë të gjitha ndryshimet e bëra në të dhëna të cilat i përpunojnë. Nuk është paraparë copëzimi i dokumentimit të tillë; duhet të jetë në përputhje me kërkesat e përgjithshme të mjaftueshmërisë.

Ekziston edhe obligimi i konfidencialitetit i përcaktuar për Kontrolluesit dhe Përpunuesit dhe për Operatorët e tyre edhe pas përfundimit të funksioneve të tyre. Asnjë Operator nuk duhet të përpunojë të dhëna personale në të cilat ai/ajo ka qasje, pa autorizim paraprak, as për çfarëdo qëllime dhe mënyrë tjetër në vend të asaj që është udhëzuar në mënyrë eksplicite.

Këto rregulla janë gjithëpërfshirëse dhe vetë-shpjeguese dhe duhet të ndiqen nga organet private dhe publike për përpunimin e të dhënave me rrezik të ulët dhe me rrezik të lartë. Secila prej këtyre dy grupeve ka obligime të ndryshme specifike të sigurisë, siç përcaktohet nga Udhëzimet Administrative dhe Rregulloret përkatëse të ASHMDHP-së (siç shpjegohet më vonë në këtë Manual).

Përpunimi i kontraktuar – kontraktimi (Neni 15)

1. Përpunuesi i të dhënave mund t'i besohet përpunimi i të dhënave personale me një kontratë të shkruar nëse ai ose ajo është i/e regjistruar në Republikën e Kosovës për të kryer veprimtari të tilla në pajtim me procedurat dhe masat e parapara me nenin 14 të këtij ligji.
2. Përpunuesi i të dhënave mund të veprojë vetëm brenda kufijve të autorizimeve të kontrolluesit të të dhënave dhe nuk mund të përpunojë të dhënat personale për qëllime tjera. Të drejtat dhe detyrimet reciproke duhet të caktohen me kontratë të shkruar, e cila po ashtu duhet të përmbajë edhe një përshkrim të detajuar të procedurave dhe masave në pajtim me nenin 14 të këtij ligji.
3. Kontrolluesi i të dhënave duhet të mbikëqyrë zbatimin e procedurave dhe masave në pajtim me nenin 14 të këtij ligji. Po ashtu, duhet të përfshijë edhe vizitat e përkohshme në lokalet ku bëhet përpunimi i të dhënave personale.

4. Në rast mosmarrëveshjeje ndërmjet kontrolluesit të të dhënave dhe përpunuesit të të dhënave, përpunuesi i të dhënave duhet menjëherë në kërkesë të kontrolluesit të të dhënave t'i kthejë të gjitha të dhënat që ai ose ajo i posedon. Përpunuesit të të dhënave nuk i lejohet t'i mbajë kopjet dhe t'i përpunojë ato më tutje.
5. Në rast të ndërprerjes së veprimtarive të përpunuesit të të dhënave, të dhënat personale duhet të kthehen menjëherë te kontrolluesi i të dhënave.

Vëmendje e veçantë i kushtohet kontraktimit pasi që po bëhet një praktikë e zakonshme në jetën ekonomike, e cila përdoret për të marrë një shërbim të jashtëm profesional jo-thelbësor për një çmim të pranueshëm në vend të përpjekjeve nga vetë Përpunuesi apo Kontrolluesi për ta bërë këtë. Me shtimin e të kontraktimit të përpunimit të të dhënave personale, evidentohet rreziku i vërtetë i sigurisë që në mënyrë efikase rezulton nga delegimi i tillë në atë nivel që do të rrezikon të drejtat e subjekteve të të dhënave. Me qëllim të parandalimit e të materializimit të kësaj në Kosovë, ekzistojnë dispozita të veçanta ligjore në lidhje me sigurinë e përpunimit të të dhënave në rast të kontraktimit të paraparë në Rregulloren mbi sigurinë e të dhënave. Është komentuar në më shumë detaje në Kapitullin 12.

Mbani në mend: - *Pavarësisht se sa shumë dhe sa larg ju kontraktoni dhe sa gjatë dhe kompleks është rrjeti i juaj i kontraktimit, ju (si Kontrollues apo Përpunues):*

- *Nuk mund t'iu shmangeni obligimeve tuaja të sigurisë*
- *Niveli rezultues i sigurisë nuk mund të degradohet, përkundrazi, duhet të përmirësohet*
- *Të gjitha palët e përfshira janë përgjegjëse për çfarëdo shkelje të sigurisë dhe përgjegjësitë e tyre të veçanta të sigurisë duhet të rregullohen në detaje me një apo më shumë kontrata me shkrim.*

Kontraktimi gjithashtu sjell një mundësi për tu kompensuar për shkelje të sigurisë në mënyrë proporcionale me dëmet reale të shkaktuara, në kundërshtim me vetë sjelljen e keqe të punonjësve (kodi i punës parasheh kufizime të rrepta mbi atë se sa dëm një punëdhënës mund të kërkoj nga punonjësi i tij). Pra, edhe pse përgjegjësia ligjore për shkak të kontraktimit nuk mund të degradohet, përgjegjësia ekonomike mundet - me kusht që:

- Kontrata e kontraktimit është formësuar në mënyrë të duhur në terme komerciale
- Kontraktuesi është i obliguar ta sigurojë veten për dështimet e mundshme për të ofruar nivel të duhur të sigurisë në rast se burimet e veta kapitale nuk janë të mjaftueshme për kompensimin e dëmeve të mundshme.

Shkelja e dispozitave për sigurinë e të dhënave personale (Neni 81)

1. Personi juridik ose personi që ushtron veprimtari të pavarur dënohet për kundërvajtje me gjobë prej katërmijë (4.000) deri në dhjetëmijë (10.000) Euro, nëse gjatë përpunimit të të dhënave personale dështon të garantojë nivel duhur për sigurimin e mbrojtjes së të dhënave personale sipas neneve 14 dhe 16 të këtij ligji.
2. Personi përgjegjës i personit juridik ose i personit që ushtron veprimtari të pavarur dënohet për kundërvajtje me gjobë prej pesëqind (500) deri në dymijë (2.000) Euro për shkelje nga paragrafi 1 i këtij neni.
3. Personi përgjegjës i organit shtetëror dënohet për kundërvajtje me gjobë prej pesëqind (500) deri në dymijë (2.000) Euro për shkelje nga paragrafi 1 i këtij neni.
4. Individi dënohet për kundërvajtje me gjobë prej dyqind (200) deri në tetëqind (800) Euro për shkelje nga paragrafi 1 i këtij neni.

4 ZMDH-ja si personi përgjegjës për sigurinë e të dhënave

ZMDH aktualisht rregullohet Ligjin nr. 03/L-172 për mbrojtjen e të dhënave personale. Ligji Nr. 03/L-172 "për Mbrojtjen e të Dhënave Personale" përcakton dispozitat në vijim mbi ZMDH-të:

Nën-kreu O - Zyrtari i Mbrojtjes së të Dhënave

Neni 74 -Zyrtari i Mbrojtjes së të Dhënave

1. Të gjitha organet publike që përpunojnë të dhëna personale zgjedhin dhe caktojnë me shkrim një zyrtari të brendshëm të mbrojtjes së të dhënave.
2. Vetëm personat të cilët posedojnë njohuri të specializuara dhe që janë të besueshëm për kryerjen e detyrës në fjalë mund të emërohen si zyrtar për mbrojtjen e të dhënave.
3. Zyrtari i mbrojtjes së të dhënave është në vartësi të kryesuesit të organit publik. Ai ose ajo nuk do të pësojë asnjë dëm gjatë kryerjes së detyrave të tij ose të saj.
4. Zyrtari i mbrojtjes së të dhënave është i detyruar të mbajë fshehtësinë e të dhënave personale, me të cilat ai ose ajo njoftohet gjatë kryerjes së detyrave të tij ose të sa.
5. Organi publik ndihmon zyrtarin e mbrojtjes së të dhënave në kryerjen e detyrës së tij ose të saj dhe duhet në veçanti në masë të nevojshme t'i vejë në dispozicion pajisjet dhe kapacitet tjera.
6. Nëse zyrtari i mbrojtjes së të dhënave nuk i përmbush më tutje kushtet e përmendura në paragrafin 2 të këtij neni, ai ose ajo shkarkohet nga detyra e tij ose e saj.

Neni 75 - Detyrat e zyrtarit të mbrojtjes së të dhënave

1. Zyrtari i mbrojtjes së të dhënave ndihmon organin publik në sigurimin se rregullat përkatëse për mbrojtjen e të dhënave janë në mbikëqyrje dhe zbatohen në mënyrën e duhur. Për këtë qëllim ai ose ajo mund ta konsultojë në çdo kohë Agjencia.

2. Zyrtari i mbrojtjes së të dhënave në mënyrë të rregullt mbikëqyrë përdorimin e duhur të programeve për përpunimin e të dhënave dhe masave e procedurave të vendosura për të garantuar përpunim të sigurt të të dhënave.
3. Zyrtari i mbrojtjes së të dhënave rregullisht i informon të gjithë personat e punësuar nga organin publik në përpunimin e të dhënave personale, me rregullat dhe dispozitat përkatëse. Ai ose ajo po ashtu rregullisht i informon të gjithë punonjësit për të drejtat dhe detyrimet e tyre sipas këtij ligji dhe rreth zhvillimeve në fushën e mbrojtjes së të dhënave.

Neni 76 - Kontrolli

1. Zyrtari i mbrojtjes së të dhënave mund të kryejë kontrolle me vetiniciativë.
2. Zyrtari i mbrojtjes së të dhënave ka të drejtë të konsultojë, të heq, të transkriptojë ose të kopjojë të dhënat personale të cilat i ndesh gjatë kontrolleve. Ai ose ajo është i/e detyruar të respektojë fshehtësinë e të dhënave personale.
3. Zyrtari i mbrojtjes së të dhënave duhet t'i raportojë me shkrim kryesuesit të organit publik për rezultatet e kontrollit.

Mbani në mend: *ZMDH është i detyrueshëm për sektorin publik dhe jo i detyrueshëm për sektorin privat*

Komentet shpjeguese shtesë - mbi drejtimet kryesore të sigurisë të dhënave që vijnë nga "Ligji nr. 03/L-172 për mbrojtjen e të dhënave personale"

Ky ligj i obligon të gjitha organet private dhe publike që përpunojnë të dhënave personale që të:

- Paraqesin masat e sigurisë të bazuara në analizën e rreziqeve dhe zbutjen e tyre përmes:
    - Aranzhimit për rrjedhën e tillë të punës së përpunimit të të dhënave ku qasja e operatorëve në të dhëna është i kufizuar në minimumin e kërkuar për kryerjen e obligimeve të tyre të punës në mënyrë korrekte,
    - Ruajtjes së integritetit dhe konfidencialitetit të të dhënave.
- Te njoftojne stafin e tyre (stafin e brendshëm dhe të jashtëm) të angazhuar në përpunimin e të dhënave në mënyrë që të jenë në gjendje t'i kuptojnë çështjet qe kane te bejne me mbrojtjen e te dhenave personale.
- Ruajnë konfidencialitetin e të dhënave edhe pas ndërprerjes së detyrës që ka lejuar qasjen e tyre. Ky konfidencialitet duhet të kuptohet mjaft gjerësisht, pasi që mbulon:
    - Vet të dhënat
    - Mjetet dhe shërbimet e përpunimit (kjo kërkesë përforcohet gjithashtu edhe nga ligjet tjera, pasi që përpunimi është një pjesë integrale e avantazhit konkurrues në ditët e sotme).
    - Masat e sigurisë të vendosura mbi dy pikat e listuara më lartë.

Këto udhëzime shumë të përgjithshme të sigurisë janë të zbatueshme për organet private dhe publike për përpunimin e të dhënave me rrezik të ulët dhe me rrezik të lartë. Këto udhëzime me të drejtë theksojnë rolin e mjeteve organizative, pasi që është shumë i vështirë dhe i shtrenjtë kompensimi i mangësive të tyre me mjete teknike. Mangësi të tilla për shkak të organizimit të gabuar të përpunimit dhe sigurisë së tij janë armiku më i madh i sigurisë së mirë. Mjetet organizative gjithashtu mbulojnë sigurinë e ndërlidhur me personel pasi që njerëzit e përfshirë në përpunimin e të dhënave zakonisht gjenerojnë dobësitë më të mëdha dhe kësisoj edhe rreziqe, dhe rreziqet e tilla nuk mund të zbuten vetëm përmes teknologjisë. Në kundërshtim me

besimin e përgjithshëm të shumë njerëzve, siç është: "të shtojmë disa gjëra më të avancuara të TIK-ut dhe problemet tona zgjidhen vetë," siguria e rezultuar në fakt mund të bëhet më keq (pasi që këto pajisje të reja të TIK-ut mund të gjenerojnë rreziqe të reja të pa-zbutura).

Kërkesa për të dhënë qasje minimale në të dhëna dhe mjetet e tyre të përpunimit është absolutisht i rëndësishëm, pasi që është një nga mjetet e mëdha për parandalimin dhe zbutjen e rrezikut. Parimi i huazuar nga fusha e përpunimit të të informatave të klasifikuara ("duhet të di") duhet të miratohet kurdo që të jetë e mundur: jepni qasjen vetëm në baza "kam nevojë të di", revokoni qasjen e tillë menjëherë kur ajo vjetrohet.

Gjithashtu kërkon njoftimin mbi sigurinë e të gjithë operatorëve. Nëse nuk zbatohet, kontrolluesit dhe përpunuesit mund të mos jenë në një pozitë solide juridike për t'i dënuar punonjësit dhe kontraktorët e tyre në rast se operatorët e tillë kanë kryer një shkelje të sigurisë, edhe në qoftë se ka qenë një akt i neglizhencës ose vetëm një budallallëk. Nëse rasti i tillë sillet para një gjykate, operatori i tillë i cili ka të drejtë ligjërisht për një trajnim të duhur, mund të fitojë rastin nëse Kontrolluesi apo Përpunuesi ka dështuar ta njoftoje atë siç duhet.

5 Rregullorja Nr. 03/2015 Mbi Masat e Sigurisë Gjatë Përpunimit të të Dhënave Personale

5.1 Obligimet e sigurisë për organet publike dhe private me rrezik të lartë dhe të ulët të parapara me rregulloren Nr. 03/2015

Arsyet e mëdha për diferencimin e organeve private dhe publike për përpunimin e të dhënave personale në aspektin e përgjegjësive dhe obligimeve të tyre të sigurisë janë:

- Balancimi i duhur ndërmjet:
  - Mbrojtjes së të drejtave të subjektit të të dhënave,
  - Vendosjes së barrës shtesë për kontrolluesit dhe përpunuesit, duke pasur parasysh rezultatin e analizës dhe vlerësimit të rrezikut.
- Pozicionimin e mbrojtjes së të dhënave personale jo si një pengesë e biznesit dhe barrë administrative dhe financiare që dëmton ekonominë, por si një vlerë të shtuar për vetë Përpunuesin apo Kontrolluesin e përpunimit të të dhënave. Informacioni i përfshirë në të dhënat personale ka gjithmonë vlerë për Përpunuesin apo Kontrolluesin (vlera e tij minimale është kostoja e mbledhjes së tij dhe përpunimit të kërkuar për ta vënë atë në dispozicion) dhe duhet të mbrohet jo vetëm për përmbushjen e obligimeve ligjore, por për arsye të shëndosha ekonomike.

Një vlerësim fillestar i rrezikut ndihmon qartë në identifikimin e atyre organeve private dhe publike ku përpunimi i të dhënave të tyre duhet të mbrohet duke përdorur një regjim më të formalizuar dhe më mirë të pajisur, duke rënë kështu në kategorinë me rrezik të lartë.

Prezantimi i një ndarje të tillë rezulton në një transparencë më të madhe dhe në realizëm ekonomik. Kërkesa nga Përpunuesi apo Kontrolluesi me rrezik të ulët që të prezantojë një sistem të plotë të menaxhimit të sigurisë së informacionit (të cilin ata nuk do ta kuptojnë plotësisht dhe nuk do ta zbatojnë për arsye ekonomike) do të ishte një qasje shumë e keqe, në kundërshtim me idenë e sigurisë së të dhënave personale.

Në mënyrë që të mbulohet i gjithë spektri i përpunimit të të dhënave, si publike dhe private, përdoret koncepti i Përpunuesit apo Kontrolluesit të përpunimit të të

dhënave; ai mbulon Kontrolluesit dhe Përpunuesit e të gjitha llojeve, duke përfshirë nën-përpunuesit.

Ndarja rezultuese e organeve publike dhe private për përpunimin e të dhënave me rrezik të lartë dhe rrezik të ulët hartohet si në vijim:

- **Organet private dhe publike me rrezik të lartë** janë organe publike dhe private për përpunimin e të dhënave që përmbushin njërin nga kushtet e mëposhtme:
    - përpunojnë të dhëna personale në lidhje me më shumë se 100 subjekte të të dhënave përgjatë një periudhe të pandërprerë 12 mujore;
    - përpunojnë kategori të veçanta të të dhënave personale, siç referohen në nenin 2, paragrafin 1.16 të Ligjit për mbrojtjen e të dhënave personale, të dhënat mbi vendndodhjen ose të dhënat mbi fëmijët ose të punësuarit në sistemet e dosjeve me një shkalle të gjerë;
    - kryejnë profilizime për të cilat masa mund të krijojnë efekte juridike në lidhje me individin ose në mënyrë të ngjashme prekin individë në masë të konsiderueshme;
    - përpunojnë të dhëna personale mbi ofrimin e kujdesit shëndetësor, hulumtimet epidemiologjike, ose hulumtime të sëmundjeve mendore ose infektive, ku të dhënat përpunohen për marrjen e masave ose vendimeve në lidhje me individë të veçantë në një shkallë të gjerë;
    - bëjnë monitorimin e automatizuar të zonave me qasje publike në një shkallë të gjerë;
    - kryejnë operacione të tjera të përpunimit për të cilat kërkohet konsultim i zyrtarit të mbrojtjes së të dhënave apo Agjencisë në pajtim me nenet 56 dhe 75 të Ligjit për Mbrojtjen e të Dhënave;
    - kur një shkelje e të dhënave personale mund të ndikojë negativisht në mbrojtjen e të dhënave personale, privatësisë, drejtave ose interesave legjitime të subjektit të të dhënave;
    - aktivitetet kryesore të kontrolluesit ose përpunuesit përbëhen nga operacionet e përpunimit të cilat, për shkak të natyrës së tyre, qëllimit dhe/ose qëllimeve të tyre, kërkojnë monitorim të rregullt dhe sistematik

të subjekteve të të dhënave;

- kur të dhënat personale janë të qasshme për një numër të personave të cilët në mënyre të arsyeshme nuk mund të jenë të kufizuar.

- **Organet private dhe publike me rrezik të ulët** janë të gjitha organe private dhe publike për përpunimin e të dhënave personale. Një ndarje e tillë në mënyrë themelore ndjek qasjen e Rregullores së Përgjithshme të hartuar rishtazi mbi Mbrojtjen e të Dhënave (RrPMDh). Merr parasysh përvojën Evropiane dhe madhësinë e Kosovës si vend, përderisa kriteret origjinale modifikohen paksa.

Ky grup i kritereve është gjithashtu shumë i arsyeshëm përmes përdorimit në shumë vende të filtrit "shkalla e madhe," pasi që lejon shmangien e zgjidhjeve të pamenduara në situatat e përpunimit kur rreziqet aktuale ndaj privatësisë nuk janë të larta. Supozon se sa më e madhe që të jete shkalla e përpunimit, më shumë rreziqe gjeneron; pasi që një shkallë e tillë e madhe zakonisht është e ndërlidhur me më shumë rrjedha më të komplikuara të përpunimit. Është nën diskrecionin e ASHMDHP-së të nxjerrë udhëzime mbi atë se si do të kuptohet në të vërtetë shkalla e "madhe" për sektorë të ndryshëm si dhe aranzhimet e përpunimit.

Çdo grup i tillë i kritereve është i diskutueshëm për ato organe private dhe publike të cilat janë në aërsi të vijës kufitare dhe ky është një problem i përgjithshëm për klasifikimin e çdo 2-kategorive. Duke qenë të vetëdijshëm për këtë dobësi sistematike, kjo dukuri është e ngjashme për të gjitha vendet e BE-së përderisa miratojnë RrPMDh-në e BE-së të hartuar rishtazi. Në rast se versioni i kritereve të miratuara së fundmi në RrPMDh do të jetë ndryshe nga sa duket më e mundshme tani, grupi i mësipërm i kritereve në legjislacionin e Kosovës duhet të rregullohet në mënyre të duhur në të ardhmen. Diskutimi legjislativ i RrPMDh-së në vazhdim është se si të formësohet kjo ndarje në mënyrë të duhur për të balancuar të drejtat e subjektit të të dhënave, sigurinë e ekonomisë, si dhe barrën e kostos dhe atë administrative të vendosur mbi organet publike dhe private për përpunimin e të dhënave sipas obligimeve të sigurisë.

5.2 Obligimet për organet publike dhe private që përpunojnë të dhëna me rrezik të ulët

Organet private dhe publike me rrezik të ulët të përpunimit të të dhënave i nënshtrohen një grupi të kufizuar dhe gjithëpërfshirës të rregullave që duhet ndjekur. Dispozitat në lidhje me sistemet e sigurisë së TIK-ut janë të detyrueshme vetëm për ato organe private dhe publike që përpunojnë të dhënat personale në mënyrë elektronike. Organet private dhe publike që përpunojnë të dhëna në mënyrë elektronike konsiderohen ato që përpunojnë çfarëdo të dhëna përmes mjeteve elektronike. Për organet private dhe publike që përpunojnë të dhëna personale në mënyrë manuale janë të zbatueshme vetëm dispozitat në lidhje me përpunimin e tillë.

Rregullorja përcakton standardet minimale për sigurinë e të dhënave personale, e cila përfshinë:

1. Analizën dhe vlerësimin e rreziqeve të thjeshtësuara – që kryhet në mënyrë periodike për të identifikuar dobësitë dhe rreziqet më të mëdha të sistemeve që ekspozohen tek ata dhe dokumentimin e tij në atë mënyrë që është e kuptueshme or praktikën e zakonshme të biznesit të këtyre organeve publike dhe private në sektorin e veçantë të ekonomisë.
2. Sigurinë fizike dhe mjedisore
3. Sigurinë logjike të pajisjeve të TIK-ut, të përdorur për përpunimin e të dhënave personale
4. Sigurinë organizative, duke përfshirë sigurinë e stafit (faktori njeri).

Dispozitat e kësaj rregullore për organet publike dhe private me rrezik të ulët formësohen në atë mënyrë që dispozitat e saja të mëdha mund të shndërrohen lehtësisht në 2 lista:

1. Detyrat dhe aktivitetet e sigurisë që duhet të kryhen
2. Lista e thjeshtë kontrolluese e pajtueshmërisë për vetë-vlerësimin e pajtueshmërisë (shih shtojcën përkatëse).

Në kundërshtim me dispozitat e Rregullores për organet publike dhe private me rrezik të lartë, një Sistem i Menaxhimit të Sigurisë së Informacionit (SMSI) që është i zhvilluar plotësisht nuk është i detyrueshëm për ta. Përkatësisht, këshillohet formësimi i të gjitha procedurave të sigurisë për një Përpunues apo Kontrollues me rrezik të ulët duke përdorur një gjuhë të thjeshtë, p.sh. duke iu referuar terme specifike të biznesit të përdorura nga sektori i Përpunuesit apo Kontrolluesit. Një qasje e tillë është shumë e dobishme në mënyrë që të bëhet i lehtë zhvillimi i procedurave të tilla të sigurisë, të kuptuarit dhe pranimi i tyre si një ndihmë e dobishme dhe jo një barrë dhe ekzekutimi i tyre pa pengesa serioze dhe pa mbikëqyrje shtesë. Këshille e mirë për personat përgjegjës për zhvillimin dhe mirëmbajtjen e procedurave të tilla është që t'i kontrollojnë ato gjatë trajnimit nëse ato janë kuptuar me të vërtetë nga ana e operatorëve të zakonshëm dhe personave tjerë përgjegjës për sigurinë e të dhënave.

Ekziston gjithashtu edhe një grup i veçantë i masave të sigurisë fizike dhe mjedisore të përcaktuara për organet private dhe publike që përpunojnë të dhënat personale në mënyrë manuale. Ato zbatojnë kontrollin e duhur të qasjes fizike dhe theksojnë shkatërrimin në kohë apo anonimizimin kur kalon periudha e mbajtjes së të dhënave. Të gjitha dokumentet rezervë në letër që janë bartës të tillë të të dhënave duhet të shkatërrohen.

Të gjitha mjetet dhe shtigjet për transmetimin e të dhënave apo dokumenteve që përmbajnë të dhëna personale duhet të enkriptohen. Gjithashtu, të gjitha mediumet portative elektronike të përdorura si bartës të informacionit (USB memorie, mediume tjera me flash memorie) duhet të enkriptohen para se të largohen nga objektet e Përpunuesit dhe Kontrolluesit që përpunojnë të dhënat.

5.3 Obligimet për organet publike dhe private që përpunojnë të dhëna me rrezik të lartë

Për dallim nga organet private dhe publike me rrezik të ulët, ato me rrezik të lartë rekomandohet të ndjekin rregullat që dalin nga standardet teknike të sigurisë së informacionit ISO-27000, edhe pse Rregullorja nuk e bën të obligueshme pajtueshmërinë e tyre. Rregullorja gjithashtu specifikon rregullat e bashkëpunimit në mes të organeve private dhe publike më rrezik të lartë dhe ASHMDHP-së për qëllime të inspektimeve dhe gjatë raportimit të shkeljeve të sigurisë.

Rregullorja paraqet Politikën e Sigurisë së Informacionit (këtu e tutje "PSI"), si dokument kryesor në të cilin Kontrolluesi apo Përpunuesi I të dhënave I njofton punonjësit dhe kontraktuesit me obligimet.

PSI-ja duhet të zhvillohet dhe të mirëmbahet në pajtim me rregullat e sigurisë së informacionit, siç parashihet me legjislacionin vendor dhe me legjislacionin e ratifikuar ndërkombëtar, të rekomanduar nga standardet e përcaktuar të sigurisë, si dhe rekomandimet e lëshuara nga ASHMDHP-ja. Analiza dhe vlerësimi i rreziqeve është një pjesë integrale e PSI- së. Dokumenti i PSI-së duhet të përcaktojë qartë objektivat e sigurisë dhe të përcaktojë masat teknike dhe organizative të nevojshme për zbutjen e rreziqeve që ndikojnë në sistemet e dosjeve për shkak të kërcënimeve dhe dobësive të identifikuara.

6 Obligimet kryesore të sigurisë gjatë kontraktimit të përpunimit të të dhënave personale

Shumica e këtyre obligimeve janë të ligjshme dhe jo teknike. Kjo është e qartë sidomos në situata të tilla kur qëllimi kryesor i transferimit nuk është reduktimi i kostos, por kryerja e përpunimit në një mënyrë më profesionale dhe/ose më të sigurte - më profesionale në aspektin e:

- Harduerit dhe softuerit që duhet të vendoset
- Shërbimeve tjera të përpunimit (sikurse transmetimi i bartësve të të dhënave fizike, arkivimi, asgjësimi i mediumeve, etj)
- Cilësia e sigurisë së ofruar – atëherë përpunuesi në këto kushte është më profesional se sa kontrolluesi, pra përpunuesi është një burim i vërtetë i ekspertizës reale, ndërsa gjërat do të organizohen në detaje.

Mbaj në mend - *Në rast të kontraktimit, ZMDH ndërhyn në një marrëdhënie kontraktuale me përpunuesin. Prandaj, një kontratë kontraktimi duhet të parashikoj një përfshirje të tillë për të bërë të mundur dhe të rezultojë në disa dispozita kontraktuale, p.sh. në ato të cilat kanë të bëjnë me aftësinë praktike të ZMDH-së për të vlerësuar sigurinë e përpunimit të të dhënave në bazë, duke përfshirë qasjen e kushtëzuar në ambientet e saj, rrjetet e TIK-ut, personelit etj. Në rast se përpunuesit e përpunimin të të dhënave do të auditohen, kontrata shumë saktësisht duhet të specifikojë dy meritat dhe kushtet organizative-teknike të auditimit, si dhe shpenzimet financiare të ndërlidhura. Në rast të mos bërjes si duhet të kësaj, mund të rezultojë në një ngërç ligjor dhe financiar, duke bllokuar një auditim të tillë. Një vështirësi shtesë në aspektin praktik vjen nga dispozitat e ligjit për mbrojtjen e të dhënave e lejuar për qasje të tillë dhe në mënyrë ad-hoc, pasi kjo është një sfidë kontraktuale në një situatë kur secila qasje e tillë potencialisht mund të rezultojë në trazira të padëshiruara tek përpunuesi. Duhet të bëhet e qartë se çfarë do të thotë teknikisht ad-hoc , pasi kjo ndikon rëndë në aspektet financiare të një kontrate shpërndarëse.*

ZMDH sigurohet që një inventar (katalog) i sistemeve arkivuese të të dhënave personale të përpunuar nga Përpunuesi apo Kontrolluesi i Përpunimit të dhënave, është mirëmbajtur në mënyre të duhur. Kjo paraqet një detyrim për të mbajtur të gjithë dokumentacionin e azhurnuar. Si e tillë, detyra është mjaft e mundimshme për çdo

Përpunues ose Kontrollues më të madh; duhet të vlerësohet në aspektin e ngarkesës se punës. Pasi që ZMDH-ja funksionon këtu më shumë si një auditor sesa një pozitë ekzekutive (detyrë e tij kryesore është mbikëqyrja, kësisoj duke hequr dorë nga të bërit vetë çdo gjë), ai / ajo nuk është i detyruar për të bërë dhe të mbaj të gjithë dokumentacionin e tillë personalisht, sidomos kur komponentët e konsiderueshëm të dokumentacionit të tillë tashmë ekzistojnë në vende të ndryshme tek Përpunuesi apo Kontrolluesi (p.sh. një inventar i plotë i mjeteve të TIK-ut në përdorim - në departamentin e TIK-ut, pasi kjo është një domosdoshmëri për arsye të prokurimit). Përpunuesi apo Kontrolluesi me rrezik të lartë, ku pjesa më e madhe e dokumentacionit të tillë është tashmë në vend, duke u ruajtur dhe mirëmbajtur nga disa njësi tjera organizative (p.sh. siguria, përputhshmëria, TIK-u, ose disa departamente të biznesit), kështu që nuk ka asnjë arsye për të kopjuar atë . Pastaj rregullat e bashkëpunimit të duhur, të drejtat e qasjes, dhe lidhjet do të vendosen në vend të përsëritjes së resurseve të mëdha të cilat janë përherë në ndryshim. Do të zbatohen rregullat e ndryshimit të menaxhimit; ato mund të huazohen nga një metodologji e menaxhimit të projektit që është më e përshtatshme për Përpunuesin apo Kontrolluesin.

Ne rast të delegimit të përpunimit të të dhënave personale, është e nevojshme të:

- Krijohen rregullat lidhur me komunikimin ndërmjet kontrolluesve dhe përpunuesve - posaçërisht në situatat emergjente si shkelja e të dhënave, përpunimi i zbërthimit, kryerja e inspektimeve të ASHMDHP-së dhe kërkesat tjera lidhur me sigurinë, si dhe njoftimi i ASHMDHP-së për arsye tjera atëherë kur sigurimi i të dhënave është kompromentuar: në emër të Kontrolluesit, apo në bashkëpunim të ngushtë me Kontrolluesin.
- Adoptimi i kornizës standarde kontraktuale që duhet të përdorin palët për delegime të tilla të përpunimit (kontrata kryesore, klauzolat kryesore, etj.).

Mbani në mend! - *Rekomandohet fuqishëm që të elaborohet një Forme e Kontratës Kryesore për kontraktimin e përpunimit të të dhënave personale tek kompania e tretë, veçanërisht në rast se:*

- *Keni përpunues të shumtë*
- *Ballafaqoheni me ndryshime të shpeshta të përpunueseve*

Ne mënyre që të sigurohet një përzgjedhje e mirë e përpunueseve, kontrolluesi duhet të merr parasysh çështjet e mëposhtme të sigurisë:

- Përzgjedhja e kompanisë që ka reputacion të mirë profesional në këtë fushë, dhe e cila ofron garanci të besueshme për sigurinë e të dhënave që do të përpunohen;
- Kontrata me përpunues duhet gjithmonë të jetë në formë të shkruar dhe të ketë dispozita veçanta që rregullojnë sigurinë e të dhënave personale;
    - Përgjegjësia e përpunuesit është gjithnjë e kufizuar vetëm në atë se çfarë thotë kontrata, dhe jo në atë se çfarë kontrolluesi mendon se është e qartë, natyrore, etj.,
    - Çdo gjë (në aspektet e përgjegjësisë dhe llogaridhënies së mundshme) e cila nuk është specifikuar në kontratë, mbetet ekskluzivisht tek kontrolluesi, duke përfshire edhe gjërat të cilat nuk mund të ndikojnë direkt për shkak të delegimit të përpunimit.
- Në rast se përpunuesi është një kompani e huaj, kontrolluesi siguron se vendet ku operon përpunuesi janë vende të cilat ofrojnë mbrojtje adekuate të të dhënave personale sipas ligjit të Kosovës. Kontrolluesi duhet t'i referohet listës së vendeve që ofrojnë mbrojtje adekuate (sipas nenit 53 dhe 54 të ligjit për mbrojtjen e të dhënave).
- Kontrolluesi siguron se përpunuesi ofron masat e duhura të sigurisë për të dhënat që duhet të përpunohen.

Kjo rregullore e ASHMDHP-së për sigurinë e të dhënave gjithashtu merr parasysh realitetin bashkëkohor të përpunimit të dhënave në ngritjen e tendencës së nën-përpunimit;

- Zakonisht sa më i madh dhe më profesional të jetë kontrolluesi, aq më shumë tenton që të kontraktoje vet-vetën, shembull: aktivitetet e veta jo-thelbësore të përpunimit të dhënave të biznesit. (posta, futja e të dhënave. etj).
- Do të ishte jo reale dhe ekonomikisht e dëmshme që thjesht të ndalohen aktivitetet e tilla

Mbani në mend: - *Kontraktimi, në çdo rast, nuk duhet të kompromet oj nivelin e sigurisë – duke rene më poshtë sesa është dakorduar ndërmjet kontrolluesit dhe kompanisë së kontraktuar.*

7 Këshilla për të mirëmbajtur dokumentacionin e përpunuar dhe sigurimin e të dhënave

Mirëmbajtja e sigurisë së dokumentacionit është një ndër sfidat më të mëdha për ZMDH-të, madje edhe në rastet kur ai / ajo ka sukses në delegimin e kësaj pune mes palëve bashkëpunuese, dhe kufizon rolin e tij / saj vetëm në mbikëqyrje. Kjo është e vërtete pasi që ata të cilat janë të emëruar si ZMDH zakonisht janë të stërngarkuar.

7.1 Mbajtja e të gjitha shënimeve të sistemeve të arkivimit dhe sistemeve të TI-së

Mbajtja e dokumentacionit të azhurnuar të të gjitha rrjedhave të përpunimit në një institucion (në ditët e sotme zakonisht janë duke kaluar në ndryshimeve të vazhdueshme) shpesh trajtohen si detyrë me prioritet sekondar, dhe në disa raste madje edhe neglizhohen. Në mënyre që ZMDH-të të funksionojnë me sukses në një ambient të tillë, kërkohet një qasje e rreptë metodologjike dhe e disiplinuar, e cila është përshkruar më poshtë. Kjo duket e thjeshtë, dhe duhet të prezantohet si e tillë në mënyre që të mos ti ndaj ato nga të qenit palë të mundshme bashkëpunuese. Kërkohet përdorimi i ciklit klasik PDCA Deming Cycle (Planifiko –Bëj – Kontrollo– Vepro) për hapat në vijim:

- Identifikimi i "procesit të biznesit" duke përfshirë përpunimin e të dhënave personale
- Identifikimi i kategorive të të dhënave personale që janë tanimë të përpunuara
- Krijimi i procedurave të veçanta për të dhënat e ndjeshme (kontrollim-paraprak, lidhëza, etj.)
- Gjurmimi i të gjitha formave të përpunimit manual (bazuar në letër)
- Dokumentimi i të gjitha të gjeturave tuaja duke krijuar magazina aktuale (katalogë) :
    - Sisteme arkivuese
    - Sisteme të përpunimit të TI-së
    - Manuale—vetëm procese të përpunuara
    - Rrjedhat e përpunimit

- Procedura përcjellëse - rafinimi i të gjeturave dhe krijimi i procedurave për përditësim

7.2 Identifikimi i proceseve të biznesit që përfshin përpunimin e të dhënave personale

Termi "proces i biznesit" shpesh është përdorur në analizat funksionale të sistemit përpunues të informatave. Qëllimi i vetëm i një analize të tillë është që të strukturohen të gjitha përpunimet e bëra nga një Përpunues ose Kontrollues në kornizën e rrjedhave të bashkëpunimit koherent të përpunimit - secila nga këto rrjedha është proces në vete. Në rast të një institucioni më të madh, struktura e përgjithshme e përpunimit mund të jetë mjaft komplekse. Në mënyrë që të ruaj përshkrimet e kuptueshme, zakonisht propozohet një grup i një liste të strukturave hierarkike. Kjo do të bëhet e kuptueshme sidomos kur parakusht i saj është delegimi i një pjese të mirëmbajtjes së inventarëve për ata që janë përgjegjës në një kuptim në "mënyrë të natyrshme" - p.sh. sipas ndarjes së punës brenda një Përpunuesi apo Kontrolluesi. Nuk ekzistojnë detyrime ligjore se si saktësisht duhet të strukturoren këto magazina, në përjashtim të një strukture detyruese (minimale) të sistemit të arkivimit të quajtur katalog. Kriteri vlerësues se sa skedare PDF duhen për të kryer një detyre mbikëqyrëse të ZMDH-së në mënyre sa më të lehtë të mundshme, kësisoj duke shmangur tepricat dhe përsëritjet e padëshiruara.

Ekzistojnë rregulla të thjeshta në vazhdim që bëjnë identifikimin e "proceseve të biznesit":

- Studimi i të gjitha ligjeve të veçanta sektoriale në dispozicion dhe dokumentacioni i brendshëm statutor i Kontrolluesit apo Përpunuesit: zakonisht përshkruan se si do të kryhen detyrat statutore. Nga kjo mund të zbulohet se çfarë mjeti i informacionit kërkohet për të përmbushur këto detyra.
- Trajtimi i këtyre detyrave statutore si një fillim i mbarë për listën fillestare të "proceseve të biznesit".
- Identifikimi i "pronarëve" (personave përgjegjës, akterëve të mëdhenj, etj.) të cilët vendosin për përpunimin e të dhënave për secilin nga këto detyra statutore: kërkoni ndihme nga njësitë e BNj dhe TIK-ut.
- Gjeni ata të cilët janë përgjegjës për mjetet e tyre të përpunimit- posaçërisht të rëndësishëm në rast se ata nuk janë të njëjtë me "pronaret" e këtyre detyrave, fatkeqësisht mund të ndodhë të mos jenë të vendosur në departamentet e TIK-ut.

- Duke pasur parasysh këto gjetje, ktheni listën e detyrave dhe mjeteve të TIK-ut në listën e proceseve të cilat nuk mbi- vendosen. Nëse jeni avokat dhe nuk keni njohuri për strukturën aktuale të vendosur të TIK-ut, kërkoni ndihme nga TIK.

Rafino listën e proceseve duke i ndarë ato në dy entitete të ndara, sipas kritereve në vijim:

- Secili prej tyre do të ketë një qëllim të veçantë (ose një grup koherent të qëllimeve) për përpunimin e tyre.
- Fushëveprimi i të dhënave të përpunuara dhe mjeteve të TI-së mund të mbi-vendosen, edhe pse shkalla e mbivendosjes do të minimizohet.
- Të përsëritet ushtrimi i tillë deri sa të përfundojë me listën e cila përmban më së shumti 3-10 procese në mënyrë tipike. Një limit pragmatik i proceseve këshillohet të përdoret këtu për arsye thjesht menaxheriale – mirëmbajtjen e çdo përshkrimi është i lidhur me disa ngarkesa të punës, dhe kjo ngarkesë e punës mund të jetë e konsiderueshme. Është e vlefshme të kufizohet një numër i proceseve në mënyrë që të bëjë këtë përshkrim koherent me analizën e mundshme të proceseve kritike, ndërsa bëhet përgatitja e vazhdueshme e planit.

7.3 Identifikimi i kategorive të të dhënave personale duke siguruar një trajtim të veçantë për të dhënat e ndjeshme

Kjo detyrë është vendimtare për plotësinë e inventarit e cila përcakton të gjithë zbatueshmërinë e saj të ardhshme si një mjet i besueshëm për çdo kontrollim të ardhshëm të përputhshmërisë. Pas identifikimit të fushëveprimit të përgjithshëm të të dhënave që përpunohen, të shqyrtohen gjetjet tuaja edhe një herë në mënyrë që të identifikohen proceset në të cilën ju përpunoni të dhënat "e ndjeshme". Nëse ato janë pjesë e një rrjedhe të gjerë të përpunimit, ju mund të largoni atë nga një rrjedhë e tillë dhe duke i ndarë ato. Qëllimi kryesor për këtë është se të dhënat “e ndjeshme" janë subjekt i kufizimeve të shumta të përpunimit dhe masave shtesë të sigurisë. Pra, ajo mund të jetë e dobishme (nga aspekti tipik menaxherial) për t’i veçuar ato si rrjedha të veçanta të përpunimit, dhe ndoshta - si sisteme të ndara të arkivimit. Ajo gjithashtu

thjeshton të gjitha auditimet e ardhshme, inspektimet si edhe shërbimet e ASHMDHP-së si dhe të gjeturat e të dhënave. Për fat të mirë, ligji për mbrojtjen e të dhënave në Kosovë në mënyrë eksplicite kërkon "etiketimin" e duhur të këtyre të dhënave, në mënyrë që të dallohen lehtësisht nga të dhënat e "zakonshme" personale. Rregullorja për sigurinë e të dhënave në mënyrë eksplicite parasheh grupe të ndryshme të dispozitave shtesë të sigurisë për të dhëna të tilla, si për përpunim automatik ashtu edhe për manual. Një nga drejtimet më të rëndësishme është ndalimi i përpunimit të të dhënave të ndjeshme në mediume portative, me përjashtim të situatave të jashtëzakonshme (të cilat në parim do të shërbehen dhe dokumentohen në mënyrë speciale).

7.4 Gjurmimi i të gjitha formave të përpunimit manual (bazuar në letër)

Format kryesore të përpunimit manual janë:

- Menaxhimi i bazuar në letër i magazinës së informacionit (kur të gjitha proceset e futjes së të dhënave dhe proceset dalëse janë kryer në mënyre manuale)
- Menaxhimi i arkivave të bazuar në letër, duke përfshirë edhe shtypjet të cilat janë përpunuar në mënyrë manuale (të nënshkruara, etj)
- Futja e të dhënave nga dokumentet në letër në sistemin e TIK-ut.
- Posta konvencionale.

Ka edhe disa forma të përpunimit të cilat përdorin bartës të të dhënave në letër që do të trajtohen si të automatizuara, shembull i mirë janë shtypjet të cilat pastaj janë shkatërruar fizikisht, pas përdorimit për përpunim të përkohshëm në formë jo-elektronike.

Rregullorja për sigurinë e të dhënave parasheh një sërë masash shtesë të sigurisë për organet publike dhe private të rrezikut lartë të cilat janë në shënjestër për parandalimin e rrjedhjes së të dhënave të dokumenteve të tilla dhe për të ndihmuar gjurmimin e lehtë të autorëve. Më të rëndësishmet janë kërkesat për një menaxhim qendror të gjithë printerëve, dhe aplikimin e burimeve identifikuese të shenjave ujore / emetuesi të çdo shtypje. Gjurmimi i të gjitha formave të përpunimit manual ju ndihmon të zbuloni mospërputhje të tilla si futja e printerëve lokale, pa informimin e

TIK-ut. Ngjarja e tillë gjithashtu zbulon një mangësi tjetër: në qasjen e menaxhimit të të drejtave: një përdorues i zakonshëm i ndonjë sistemi të TIK-ut do të ndalohet nga instalimi i ndonjë pajisje të re.

7.5 Dokumentacionet relevante

Dokumentimi i të gjitha të gjeturave tuaja duke krijuar depo aktuale është hapi tjetër logjik. Nuk ka asnjë formë të detyrueshme për një dokumentacion të tillë (përveç strukturës së katalogut për secilin sistem të të dhënave personale të arkivuara). Megjithatë, është e rëndësishme që ky dokumentacion duhet të mirëmbahet në mënyrë të përgjegjshme (ashtu që kërkon një "ndryshim të sistemit të menaxhimit" – nënkupton kontroll të versionit në formën e tij më të thjeshtë). Ajo gjithashtu duhet të bëhet në një formë që mund të komunikohet me sukses tek ata që janë të përfshirë në furnizim me informacion të nevojshëm, dhe në përdorim për arsye të tjera të ndryshme (auditimit, aplikacione të përpunimit të të dhënave', etj). Pra, një formë elektronike është praktikisht zgjidhja e vetme.

Pas përfundimit të ushtrimeve të listuara më lart, secila rrjedhë e përpunimit mund të përshkruhet në terme të katalogut të sistemit të të dhënave, siç keni identifikuar me sukses secilin nga këto rrjedha të përpunimit:

- Baza ligjore për përpunimin e tij (kategoritë e ndara "të ndjeshme" dhe "jo-të ndjeshme" të të dhënave personale)
- Qëllimi(-et) i përpunimit të saj
- Fushëveprimi i përpunimit të dhënave personale (vargu i të dhënave)
- Periudhat e përpunimit (periudhat e ruajtjes së të dhënave)
- Mjetet e TIK të caktuara për këtë përpunim
- Kujt munden/duhet t'i shpalosen të dhënat, duke përfshirë transferimet ndërkombëtare.
- Duke pasur parasysh këtë, dy magazinat (dhe përshkrimet e tyre të ndër-lidhjes) tani mund të krijohen:
- Depo e sistemeve të arkivimit të të dhënave personale (katalogët): lista e të gjitha Sistemeve të Arkivimit të të dhënave personale të përdorura për

përpunimin e tyre, të azhurnuara.

- Depo (regjistri) i sistemeve të TIK-ut të përdorura për përpunimin e tyre, gjithashtu të azhurnuara.

Kjo jep inputin e nevojshëm për regjistrin e operacioneve të përpunimit - një magazine tjetër e ZMDH-së që duhet ruajtur (i detyrueshëm për organet publike).

7.6 Udhëzimet e rëndësishme për ZMDH-të gjatë dizajnit të inventarit (katalogëve) të sistemeve të arkivimit të të dhënave personale

Inventari i tillë është një listë që përmban pjesën përshkruese tashmë të diskutuar, e ndryshuar me gjithë informacionin e nevojshëm shpjegues. Forma e tij teknike është e lirë që të zgjidhet, në një organizatë të madhe kjo zakonisht do të rezultojë në një lloj baze të dhënash që do të kërkohet në mënyrë të lehtë për të gjetur dhe për të asociuar me proceset, sistemet, operacionet e përpunimit, përgjegjësisë ("pronarët e procesit të biznesit"), etj. Më e rëndësishme është, se një listë e tillë e të gjitha sistemeve të dosjeve të të dhënave personale duhet të mbahet e azhurnuar - çdo Përpunues ose Kontrollues bashkëkohor i përpunimit të të dhënave pëson ndryshime të përhershme të artit, dhe të punësuarit janë të inkurajuar që të jenë kreativë të cilët jo domosdoshmërish mund të jetë në linjë me disiplinën e rreptë dhe gatishmërinë për të dokumentuar siç duhet çdo ndryshim të veçantë.

Struktura e saj dhe "granulariteti (copëzimi)" (sa sisteme të arkivimit të të dhënave personale duhet të krijohen, si janë të strukturuara ato dhe të ndërlidhura me njëra tjetrën, etj.) nuk janë parapare me ligj, kësisoj duke e bërë këtë mjaft fleksibile për tu përshtatur si duhet me të gjithë rrethanat specifike të përpunimit të të dhënave. Mund të ekzistoj vetëm

një sistem i arkivimit të të dhënave personale tek sistemi i përpunimit të të dhënave të Kontrolluesit, duke mbuluar të gjitha Përpunimet e të dhënave të personale, por:

- Bën shumë të thjeshtë inventarizimin(katalogët) e sistemeve të arkivimit të të dhënave personale (përparësi).
- Mund të bëjë mbikëqyrjen më pak llogaridhënëse (mangësi).

- Mund të vështirësoj apo edhe praktikisht të paaftësoj delegimin e disa detyrave që lidhen me mirëmbajtjen e saj tek "pronarët" aktual të "proceseve të biznesit".
- Nëse të dhënat "e ndjeshme" gjithashtu janë përpunuar, kjo e bën edhe më të vështirë të dallohen regjimet mbrojtëse për të dhënat "jo të ndjeshme" dhe "të ndjeshme" kur të dhënat që përfaqësojnë këto dy kategori të ndryshme vendosen në të njëjtin sistem të arkivimit.

Mbani në mend - *Zgjidhja e rekomanduar është që të ketë më shumë se një sistem të arkivimit në Inventar, të ndarë në mënyrë të tillë që është mënyra më e thjeshtë dhe më e përgjegjshme dhe po ashtu pasqyron edhe ndarjet organizative, pasi që kjo gjithashtu thjeshtëzon ndarjen e përgjegjësive të sigurisë. Ajo duhet edhe të sinkronizohet me fushëveprimin e përpunimit të kryer nga një ose më shumë sisteme bashkë-vepruese të TIK-ut, kryerja e proceseve dalluese (BNj dhe menaxhimi i pagave, shitjes, marketingut, etj.). Gjithashtu është edhe një ide shumë e mirë që të ndahet në mënyrë të qartë procesi(-et) manual duke përdorur vetëm dokumente në letër.*

7.7 Procedura përcjellëse – rafinimi i të gjeturave tuaja, krijimi i procedurave të përditësuara për të gjitha dokumentet përkatëse

Një ndër sfidat më të mëdha të ZMDH-së është mbajtja e të gjitha këtyre magazinave të azhurnuara. Në qoftë se disa pjesë të detyrës së saj të mirëmbajtjes janë deleguar (p.sh. në departamentin e TI-së për të mbajtur listën e azhurnuar të sistemeve të TIK-ut në përdorim për përpunimin e të dhënave personale), të gjithë përgjegjësit tjerë do të vazhdojnë të vazhdojnë punën sipas të njëjtës mënyrë të dakorduar më parë.

Aktiviteti më i rekomanduar për t'u informuar në kohë dhe me saktësi është aranzhimi i një bashkëpunimi të mirë me të gjitha palët kyçe të interesuara:

- "Pronaret e proceseve të biznesit"
- BNj
- TIK
- Auditimet e brendshme, inspektimet apo pajtueshmëria (nëse është prezent).
- Më poshtë mund të gjeni disa këshilla të dobishme se si bëhen gjërat më lehtë

dhe më të kuptueshme për të menaxhuar.

- Forma e rekomanduar për mirëmbajtjen e të gjitha magazinave: në mënyrë elektronike.
- Për përdorim tuaj të brendshëm, ju mund të përdorni një version të përshtatur të formës për regjistrim të sistemeve të arkivimit të ASHMDHP-së. Nuk ka nevojë që të gjitha të jenë në letër! Ju mund të vazhdoni të mbani disa kopje në letër (p.sh. shtypjet nga një regjistër elektronik) në qoftë se ju mendoni se kjo mund të kontribuojë pozitivisht në detyrë, ose është e detyrueshme për disa arsye tjera.
- Në rast se procedurat tuaja tjera të brendshme kërkojnë një formë me shkrim për një dokumentacion të tillë (p.sh. për dokumentacionin përkatës të BNj në formë të letrës):
    - Skano dokumentin final të nënshkruar
    - Ruaj këtë skenim në magazinë elektronike
    - Indeksoni atë në katalog në mënyrë që të jetë në gjendje që të gjeni lehte manifestimet e tij (në letër dhe në formë elektronike)
    - Depozito dokumentin në letër në një vend të siguruar fizikisht – vetëm për ruajtje dhe përdorim të mundshëm në rrethana ligjore që kërkojnë formën me shkrim, jo për përdorim të përditshëm.
- Dizajno, shpërndaj dhe përdor aktivizues për të ju alarmuar mbi:
    - Skadimin e afatit të të dhënave të ruajtura
    - Datat e kërkuara/ të dakorduara për azhurnim
    - Datat e kërkuara/ të dakorduara për rishikim
- Edhe në rast se procedurat e përgjithshme për auditim të brendshëm nuk do të zbatohet drejtpërdrejte për ju:
    - Kryeni vet vlerësimet tuaja të brendshme, dhe dokumentoni ato,
    - Pyetni menaxhmentin rreth Përpunuesit apo Kontrolluesit tuaj në mënyre që të përfshijnë përputhshmërinë e mbrojtjes së të dhënave personale në planin e përgjithshëm zyrtar të auditimit.

Ruzhdi Jashari

Mbikëqyrës Kryesor Shtetëror

12 prill 2016