Projekt – twining i BE-së „Mbështetje në zbatimin e kornizës së modernizuar ligjore për mbrojtjen e të dhënave personale”

UDHËZUES PËR MBROJTJEN E TË DHËNAVE PERSONALE NË SEKTORIN FINANCIAR

Ky projekt financohet nga Bashkimi Evropian

HYRJE:

Industria financiare kalon në transformim bazik për shkak të zhvillimit të shpejtë teknologjik dhe globalizimit. Këto momente zhvillimore sollën edhe sfidë të re për institucionet financiare në formë të miratimit të masave të reja për harmonizim të legjislacionit nacional në Republikën e Maqedonisë së Veriut në lidhje me përpunimin e të dhënave personale të personave fizikë.

Edhe pse disa nga parimet themelore nga regjimi i vjetër i mbrojtjes së të dhënave personale ende nuk zbatohen, Ligji i ri për mbrojtjen e të dhënave solli disa koncepte të reja të cilat mund të kenë ndikim të konsiderueshëm mbi sektorin financiar dhe të imponojnë ndryshime në mënyrën në të cilën këto institucione i përpunojnë të dhënat personale.

Qëllimi i këtij Udhëzuesi është të sigurojë përkrahje të kontrolluesve dhe përpunuesve nga sektori financiar dhe ta rrisë vetëdijen për elementet kryesore lidhur me përpunimin e të dhënave personale nga ana e kompanive që punojnë në këtë sektor.

1. ZBATIMI MATERIAL I LIGJIT PËR MBROJTJEN E TË DHËNAVE PERSONALE

Me hyrjen në fuqi të ligjit të ri për mbrojtjen e të dhënave personale ("Gazeta Zyrtare e RMV-së" numër 42/20; në tekstin e më poshtëm: LMDHP) modernizohet regjimi ekzistues juridik në Republikën e Maqedonisë së Veriut që të merren parasysh momentet dhe sfidat e reja zhvillimore në fushën e mbrojtjes së të dhënave personale. Përveç forcimit të mëtejshëm të dispozitave ekzistuese ligjore, legjislacioni i ri përfshin edhe risi të caktuara.

Nga aspekti i përfshirjes territoriale nga neni 3, Ligji për mbrojtjen e të dhënave personale zbatohet në përpunimin e të dhënave personale nga ana e kontrolluesit ose përpunuesit të themeluar në territorin e Republikës së Maqedonisë së Veriut, pa marrë parasysh vendin ku kryhet përpunimi. Gjithashtu, dispozitat nga LMDHP zbatohen edhe në përpunimin e të dhënave personale nga ana e kontrolluesve që nuk janë themeluar në Republikën e Maqedonisë së Veriut, por janë themeluar në vend ku zbatohet e drejta e RMV-së sipas marrëveshjeve të ratifikuara ndërkombëtare në pajtim me Kushtetutën e Republikës së Maqedonisë së Veriut.

Kur të dhënat personale barten në Republikën e Maqedonisë së Veriut kontrolluesve ose përpunuesve të vendeve të treta ose organizata ndërkombëtare, niveli i mbrojtjes së subjektit të të dhënave personale që e garanton ligji nacional nuk guxon të nënçmohet, me ç'rast proces i tillë mund të kryhet vetëm nëse është i harmonizuar me LMDHP.

2. DEFINICIONI PRECIZ DHE I DETAJUAR I " TË DHËNAVE PERSONALE"

Për qëllimet e ligjit të ri, neni 4 përmban definicione të reja të cilat janë me rëndësi esenciale për zbatimin e tij. Mes tjerash, LMDHP vendos definicion preciz dhe të detajuar për çdo të dhënë që duhet të sigurojë mbrojtje sa më të gjerë për subjektet e të dhënave personale dhe mund të jetë e rëndësishme për rrjedhat dhe aktivitet e ardhshme të institucioneve nga sektori financiar që nënkuptojnë përpunim të të dhënave personale.

Konkretisht e dhënë personale është secila informatë që ka të bëjë me person fizik të identifikuar ose person fizik i cili mund të identifikohet drejtpërsëdrejti ose tërthorazi, veçanërisht në bazë të identifikuesve siç janë: emri dhe mbiemri, numri amë i qytetarit, të dhëna për lokacionin, identifikues nëpërmjet rrjeteve për komunikime elektronike, ose në bazë të një ose më shumë veçorive specifike për identitetin fizik, fiziologjik, gjenetik, mental, ekonomik, kulturor ose social të atij personi fizik;

3. PARIMET KRYESORE TË LIGJIT PËR MBROJTJEN E TË DHËNAVE PERSONALE

Parimet kryesore të dhëna në Nenin 9 nga LMDHP paraqesin pikënisje për çdo përpunim të të dhënave personale.

Parimet me të cilat ka të bëjë përpunimi i të dhënave personale dhe janë përcaktuar me LMDHP i përfshijnë:

3.1. Ligjshmëri, drejtësi dhe transparencë

Në pajtim LMDHP, ekzistojnë gjatë baza juridike për përpunim të të dhënave personale të paraqitura në nenin 10. Para se të fillojnë me aktivitet që i nënkuptojnë përpunimin e të dhënave personale, kontrolluesit duhet të ndajnë kohë që të përcaktojnë se cila është baza juridike adekuate për përpunimin e paraparë.

Përveç përpunimit ligjor, LMDHP imponon edhe përpunim të drejtë të të dhënave personale. Ky parim kryesisht ka të bëjë në marrëdhënien ndërmjet kontrolluesit dhe subjektit të të dhënave personale. Në esencë, kontrolluesi duhet t'i njoftojë subjektet e të dhënave personale dhe opinionin e përgjithshëm se ata do të përpunojnë të dhëna personale, dhe duhet të jenë në mundësi të demonstrojnë harmonizim të operacionit për përpunim me LMDHP. Operacionet për përpunim nuk guxojnë të zhvillohen në fshehtësi dhe subjektet e të dhënave personale duhet të jenë të vetëdijshëm për rreziqet potenciale.

Para përpunimit, kontrolluesi duhet t'i informojë subjektet e të dhënave personale për qëllimet e përpunimit dhe adresa e kontrolluesit. Informacionet për operacionet e përpunimit të të dhënave personale duhet të sigurohen në gjuhë të qartë dhe të thjeshtë që t'u mundësohet subjekteve të kuptojnë lehtë rregullat, rreziqet, masat e sigurisë, dhe të drejtat e tyre.

3.2. Kufizimi i qëllimit

Ky parim imponon çdo përpunim të të dhënave personale të bëhet për qëllim konkret i cili është definuar para fillimi të vetë përpunimit, me ç'rast çdo përpunim plotësues për qëllime tjera duhet të jetë kompatibil me qëllimin origjinal. Çdo qëllim i ri për përpunimin e të dhënave personale i cili nuk është kompatibil me qëllimin origjinal duhet të bazohet në bazë juridike të veçantë

3.3. Vëllimi minimal i të dhënave

Përpunimi i të dhënave personale duhet të jetë i kufizuar në atë që është e domosdoshme për plotësimin e qëllimit konkret. Kategoritë e të dhënave personale të cilat janë të zgjedhura për përpunim duhet të jenë të domosdoshme për arritjen e qëllimit të përgjithshëm të operacionit për përpunim.

3.4. Saktësia e të dhënave

Kontrolluesit nuk guxojnë të përpunojnë të dhëna personale nëse nuk kanë marrë hapa të arsyeshëm që të sigurohet se të dhënat personale janë të sakta dhe të azhurnuara.

3.5. Kufizimi i afatit për ruajtje

Të dhënat personale duhet të fshihen ose anonimizohen (me ç'rast ruajtja ligjore e të dhënave të cilat më nuk janë të nevojshme mund të arrihet me ruajtjen e tyre në formë në të cilën lejon identifikimin e subjektit të të dhënave personale) menjëherë sapo të mos nevojiten më për qëllimet për të cilat janë grumbulluar.

Në përgjithësi, kontrolluesit duhet të përcaktojnë afat kohor për shlyerjen e të dhënave personale dhe në mënyrë plotësuese çdo kontrollues duhet të kryejë kontrolle periodike që të sigurohet se të dhënat nuk ruhen më gjatë se ajo që është e domosdoshme.

Duke pasur parasysh se shumë aktivitete të institucioneve të sektorit financiar në cilësinë e kontrolluesit janë në pajtim me dispozitat e Ligjit për mbrojtjen e të dhënave personale, dispozitat e posaçme sektoriale përfshijnë dispozita për afatet kohore lidhur me obligimin për ruajtjen e të dhënave. Në këtë kuptim, për shembull, neni 51 nga Ligji për parandalim dhe larje të parave dhe financim të terrorizimit ("Gazeta Zyrtare" numër 120/2018, 275/2019 dhe 317/2020) përcakton se institucionet janë të obliguara t'i ruajnë të dhënat personale të klientëve të tyre për periudhë prej dhjetë vjetësh.

3.6. Siguria

Parimi i sigurisë së të dhënave personale imponon, në varësi të rrethanave konkrete të çdo rasti në veçanti, zbatimin e masave teknike dhe organizative gjatë përpunimit të të dhënave personale me qëllim që të njëjtat duhet të jenë të mbrojtura nga qasje e rastësishme e paautorizuar ose e paligjshme, shfrytëzim, ndryshim, zbulim, humbje, dëmtim ose asgjësim.

Klientët e vlerësojnë privatësinë e tyre dhe janë të brengosur për mënyrën në të cilën të dhënat e tyre personale janë të mbrojtura në kontekst të teknologjive bashkëkohore.

3.7. Llogaridhënia

Duke pasur parasysh se edhe institucionet financiare janë lëndë e detyrimeve të zbatueshme në suaza të regjimeve të ndryshme rregullatore, llogaridhënia është parim i ri që e fut korniza e re ligjore dhe, në esencë, ajo e vendos detyrimin për kontrolluesit që të zbatojnë masa të cilat i plotësojnë parimet e lartpërmendura.

4. LIGJSHMËRIA E PËRPUNIMIT TË TË DHËNAVE PERSONALE

Qëllimi i definuar dhe i përcaktuar mirë i përpunimit të të dhënave personale para se kontrolluesi të fillojë me aktivitetet për përpunim është gur themeli i regjimit për mbrojtjen e të dhënave personale.

Ekziston spektër i gjerë i qëllimit për të cilën institucionet financiare mund të përpunojnë të dhëna nga qëllimet "bazë" të cilat karakterizohen për lloje tjera të institucioneve, siç është përpunimi i të dhënave personale për qëllimet e marrëdhënieve të punës/punësimit, deri te qëllimet të cilat kanë të bëjnë në sigurimin e shërbimit për klientë ose qëllime konkrete të cilat janë në pajtim me kërkesat që dalin nga ligjet nacionale.

Siç është theksuar në Udhëzuesin për përpunimin ligjor të të dhënave personale, neni 10 nga LMDHP përcakton gjashtë baza juridike.

Në përgjithësi, pëlqimi të cilin institucionet financiare e shfrytëzonin deri në hyrjen në fuqi të ligjit të ri mund të jetë bazë juridike adekuate për përpunimin e të dhënave personale vetëm nëse janë plotësuar kushtet nga neni 11 nga LMDHP. Ligji jep edhe definicion për pëlqimin si vullnet i dhënë i lirë, konkret, i informuar dhe i qartë i

personave fizik nëpërmjet deklaratës ose veprimit të përcaktuar qartë me të cilin jepet pëlqim për përpunim të të dhënave personale të tij/saj.

Është e rëndësishme kontrolluesit të rishikojnë aktivitetet e punës dhe në mënyrë të detajuar t'i evidentojnë që të jenë të sigurt se deklaratat për pëlqim i plotësojnë standardet nga Ligji i ri për mbrojtjen e të dhënave personale.

Neni 10, paragrafi (1), alineja b) nga LMDHP përcakton se përpunimi i të dhënave personale është i ligjshëm vetëm nëse:

- përpunimi është i nevojshëm për plotësimin e marrëveshjes ku subjekti i të dhënave personale është pala e marrëveshjes, ose

- për marrjen e hapave të caktuar të kërkesës së subjektit të të dhënave personale para qasjes drejt marrëveshjes.

Kur kontrolluesit nga sektori financiar e shfrytëzojnë këtë bazë juridike përveç për përpunimin e tyre, që të përmbushet kushti për ligjshmëri të marrëveshjeve duhet të jenë valide në pajtim me të drejtën kontraktuese që zbatohet. Për shembull, kur marrëveshja lidhet me fëmijë, ajo nënkupton sigurimin e harmonizimit me ligjet nacionale të cilat kanë të bëjnë me kapacitetin juridik të fëmijëve në raport të lidhjes së marrëveshjes. Përveç kësaj, që të sigurojnë harmonizim me parimin për ligjshmëri dhe drejtësi, kontrolluesit duhet t'i plotësojnë obligimet tjera ligjore që kanë të bëjnë në marrëveshjen konkrete, për shembull, kushte lidhur me marrëveshjet me konsumatorë ose, konkretisht, lidhur me marrëveshjen për miratimin e kredive të klientëve.

Duhet të shënohet se sipas nenit 10, paragrafi (1), alineja b) nga LMDHP, element i rëndësishëm i përpunimit ligjor është koncepti i "domosdoshmërisë. Për këtë qëllim, për shembull, përpunimi i të dhënave personale për qëllimet e pengimit të mashtrimit me siguri do të përfshijë më shumë të dhëna nga ajo që është e domosdoshme për realizimin e kësaj marrëveshjeje. Prapëseprapë, përpunimi i tillë mund të jetë i domosdoshëm që institucionet financiare të arrijnë harmonizim me detyrimin juridik nga neni 10, paragrafi (1), alineja v) nga LMDHP.

Në sektorin financiar ekzistojnë disa dispozita nacionale që kanë të bëjnë me përpunimin e të dhënave personale që e kryejnë institucionet financiare, dhe nga këtu lloji i tillë i përpunimit duhet të jetë i harmonizuar me detyrimin juridik i cili është përcaktuar me ligjin që e zbaton kontrolluesi konkret. Në situatë të tillë, ligji nacional amë mund të përmbajë dispozita korrekte për përshtatjen e zbatimit të rregullave nga LMDHP dhe kushtet e përgjithshme që kanë të bëjnë në ligjshmërinë e përpunimit nga ana e kontrolluesit, siç janë: përcaktimi i kategorive të të dhënave personale që janë lëndë e përpunimit, përcaktimi i subjekteve të prekura të të dhënave personale,

përcaktimin e qëllimeve për të cilat të dhënat personale mund të zbulohet në anë tjera, kufizimi i qëllimit të përpunimit, afatet kohore për ruajtjen e të dhënave, etj.

Një shembull, për të lartpërmendurën është Ligji për parandalim dhe larje të parave dhe financim të terrorizimit ("Gazeta Zyrtare e RMV-së" numër 120/2018, 275/2019 dhe 317/2020) në lidhje me shfrytëzimin e të dhënave që janë marrë në pajtim me këtë ligj.

Neni 60

(1) Të dhënat e siguruara në bazë të këtij ligji, duke përfshirë edhe të dhënat personale, përdoren vetëm për zbulimin dhe parandalimin e pastrimit të parave dhe financimit të terrorizmit.

(2) Dorëzimi i të dhënave nga paragrafi (1) i këtij neni deri te Drejtoria për Zbulim Financiar dhe deri te organi mbikëqyrës përkatës nga neni 146 i këtij ligji gjatë kryerjes së mbikëqyrjes në pajtim me këtë ligj nuk konsiderohet se është zbulim i sekretit afarist ose zbulim i të dhënave dhe informative të klasifikuara.

(3) Të punësuarit në subjektet dhe personat të cilët udhëheqin me subjektet që kanë për obligim të ndërmarrin masa dhe veprime për zbulimin dhe parandalimin e pastrimit të parave dhe financimit të terrorizmit në pajtim me këtë ligj, nuk guxojnë t'i përdorin të dhënat personale nga dosjet e klientëve për qëllime të tjera përveç për zbatimin e masave dhe veprimeve për zbulimin dhe parandalimin e pastrimit të parave dhe financimit të terrorizmit në përputhje me qëllimet e parapara me këtë ligj.

5. TË DREJTAT E SUBJEKTEVE TË TË DHËNAVE PERSONALE

Mbrojtja e të dhënave personale nuk mund të sigurohet nëse nuk respektohen të drejtat dhe parimet e përcaktuara në ligj. Të gjitha të drejtat e subjektit të të dhënave personale dhe detyrimet e kontrolluesit dhe të përpunuesit në lidhje me lehtësimin e realizimit të të drejtave të personave fizikë të dhënat personale të të cilëve përpunohen e japin esencën e të drejtës bazike për mbrojtjen e të dhënave personale dhe zbatimi i tyre duhet të konsiderohet rregull e përgjithshme.

Të drejtat e subjektit të të dhënave personale rregullohen në Kapitullin III të LMDHP-së, me ç'rast theksi vihet në transparencën e rritur drejt subjektit të të dhënave personale dhe drejt publikut të përgjithshëm, që në instancë të fundit e kërcënon pozicionin e tyre.

Për shembull, mes tjerash, subjektet e të dhënave personale kanë të drejtë të qasjes, kurse jo vetëm të drejtë të marrin vërtetim nëse të dhënat e tyre personale përpunohen, dhe kështu, me kërkesë të subjektit, kontrolluesi është i obliguar të sigurojë kopje të të dhënave personale për atë pa kompensim.

Për këtë qëllim, kur janë plotësuar rrethana të caktuara, subjektet e të dhënave personale kanë të drejtë të marrin të dhënat e tyre personale në format të strukturuar, zakonisht të shfrytëzueshëm dhe format makinerike të lexueshëm, dhe kanë të drejtë t'ia bartin të dhënat e tilla kontrolluesit tjetër (bartja e të dhënave).

Gjithashtu, në pajtim me LMDHP, subjektet e të dhënave personale kanë të drejtë të shlyerjes së të dhënave personale të tyre. Nënkuptohet, kjo e drejtë nuk është absolute, kurse veçanërisht nuk është as nga afër fusha e rregulluar (ku zbatohen dispozitat nga ligje nacionale të posaçme) me ç'rast institucione financiare nuk do t'i shlyejnë të dhënat personale vetëm me kërkesë të parashtruar të subjektit për shkak të detyrimit për harmonizim me obligimin juridik të përcaktuar me ligj.

Shembull tjetër lidhur me shlyerjen e të dhënave personale nga ana e institucioneve financiare është rasti kur ato përpunojnë të dhënave personale të personit fizik para marrjes së hapave para hyrjes së marrëveshjes për miratim të huas. Në kuadër të procedurës për miratim të huas, institucione financiare do të duhet të përpunojnë të dhëna të caktuara që ta vlerësojnë rrezikun kreditor të aplikuesit, dhe nëse vlerësimi i tillë rezulton me vendim negativ, respektivisht huaja nuk është miratuar për personin fizik, mund të thuhet se në këtë rast nuk do të lidhet marrëveshje me aplikuesin. Në këtë kuptim, aplikuesi nuk bëhet klient dhe konsiderohet se qëllimi i përpunimit të të dhënave personale është plotësuar, për çka ruajtja e të dhënave të tilla nuk i nënshtrohet obligimeve të përcaktuara me ligje të posaçme nacionale të cilat kanë të bëjnë me ruajtjen e të dhënave personale të klientit.

Që institucionet financiare të mund të kenë mundësi t'i plotësojnë këto obligime, ato duhet që në fillim të vendosin procedura të rregullta (mes tjerash, dhe për sigurimin se shkresat, respektivisht të dhënat personale janë të sakta dhe të azhurnuara) të cilave i mundësohet të kërkojnë, të bëjnë kopje dhe t'i nxjerrin të dhënat personale konkrete që kanë të bëjnë me subjektet e prekura, ose t'i shlyejnë.

6. MBROJTJA TEKNIKE DHE E INTEGRUAR E TË DHËNAVE PERSONALE

Sipas kornizës së re juridike për mbrojtjen e të dhënave personale, institucionet financiare duhet t'i vlerësojnë rreziqet për të drejtat dhe liritë e personave fizikë nga përpunimi i paraparë i fillimit të çdo projekti të ri i cili nënkupton përpunim të të dhënave personale gjatë zhvillimit të produkteve dhe shërbimeve të reja.

Gjatë zbatimit të këtyre masave kontrolluesi duhet të marrë parasysh teknologjinë më të re ekzistuese, shpenzimet për zbatim, natyrën, vëllimin dhe qëllimet e përpunimit të të dhënave personale, si dhe rreziqet dhe ndikimin e tyre mbi të drejtat dhe liritë e subjektit të të dhënave personale.

Institucionet financiare duhet të zbatojnë masa organizative dhe teknike adekuate që të sigurojnë se për çdo qëllim konkret, sipas rregullit, përpunohen vetëm ato të dhëna personale të cilat janë të nevojshme për të njëjtën.

7. PËRPUNUESI I PËRMBLEDHJES SË TË DHËNAVE PERSONALE

Konceptet e kontrolluesit dhe përpunuesit kanë rol kryesor në zbatimin e LMDHP sepse përcaktojnë kush është përgjegjës për përputhshmërinë e rregullave të ndryshme për mbrojtjen e të dhënave personale si dhe subjektet e të dhënave personale mund të realizojnë të drejtat e tyre në praktikë.

Sipas definicionit të ligjit, përpunues i përmbledhjes së të dhënave personale është personi fizik ose juridik, organi i administratës shtetërore, organi publik, agjencia ose trupi tjetër që kryen përpunim të të dhënave personale në emër të kontrolluesit; Për këtë qëllim, ekzistojnë dy kushte bazë për një person fizik ose juridik që të kualifikohet si përpunues: të jetë entitet i veçantë në lidhje me kontrolluesit dhe të përpunojë të dhëna personale në emër të kontrolluesit.

Kontrolluesi mund të shfrytëzojë shërbime vetëm të përpunuesve të cilit sigurojnë garanci të mjaftueshme për zbatimin e masave adekuate teknike dhe organizative me

qëllim që përpunimi të plotësojë kushtet e përcaktuara me LMDHP. Elementet që duhet të merren parasysh përfshijnë:

- Njohuri profesionale të kontrolluesit (p.sh. profesionalizëm teknik në lidhje të masave të sigurisë dhe prishjen e sigurisë së të dhënave personale);
- besueshmëri të përpunuesit;
- resurse dhe përmbajtje deri te kodeksi i miratuar për sjellje ose mekanizim për certifikim nga ana e përpunuesit.

Çdo përpunim i të dhënave personale nga ana e përpunuesit duhet të rregullohet me marrëveshje ose akt tjetër të përgjithshëm në formë të shkruar dhe elektronike, dhe me karakter obligativ. Kontrolluesi dhe përpunuesi mund të zgjedhin të negociojnë për kushtet e tyre të ndërsjella të marrëveshjes, duke përfshirë edhe të gjitha elementet e detyrueshme të marrëveshjes së tillë, ose mund të bazohen, pjesërisht ose tërësisht, në marrëveshjet me klauzola standarde.

LMDHP i përcakton elementet të cilat duhet t'i përmbajë marrëveshja për përpunimin e të dhënave personale. megjithatë, marrëveshja e tillë nuk guxon t'i përshkruajë dispozitat e ligjit. Përkundrazi, ajo duhet të përfshijë informata konkrete dhe specifike për atë se si do të plotësohen kushtet dhe cili nivel i sigurisë është i nevojshëm për punimin e të dhënave personale që është lëndë e marrëveshjes.

Detyrimi për shfrytëzimin e shërbimeve vetëm nga përpunues të cilët "sigurojnë garanci të mjaftueshme", ashtu siç janë dhënë në nenin 32 të LMDHP-së, është detyrimi ekzistues dhe prandaj kontrolluesi duhet t'i kontrollojë kufijtë e përpunuesit në intervale adekuate duke përfshirë edhe nëpërmjet kontrolleve dhe shqyrtimeve, kur është adekuate.

8. EVIDENCA PËR AKTIVITETET E PËRPUNIMIT

LMDHP-ja përcakton detyrim për ekzistimin e dokumentacionit të shkruar dhe pasqyrë të procedurave për përpunimin e të dhënave personale. Shkresat për aktivitetet për përpunim duhet të përfshijnë informacione për përpunimin e të dhënave personale, duke përfshirë edhe kategori të të dhënave personale, grupin e subjektit të të dhënave personale, qëllimin e përpunimit dhe shfrytëzuesit e të dhënave personale. Me kërkesë, kjo evidencë duhet të vihet në dispozicion të AMDHP.

Në pajtim me nenin 32, paragrafin (2) të LMDHP-së, obligimi për mbajtjen e evidencës për aktivitet për përpunim nuk ka të bëjë vetëm me kontrolluesin dhe përfaqësuesit e tij, por edhe të përpunuesit dhe përfaqësuesit e tij.

Çdo kontrollues është përgjegjës të mbajë evidencë për të gjitha aktivitetet për përpunim të cilat zhvillohen në organizatë. Këto evidenca (të cilat duhet të jenë në formë të shkruar dhe elektronike) duhet të përmbajnë informacionet si vijojnë:

- emër dhe kontakt të detajuar të kontrolluesit dhe të oficerit për mbrojtjen e të dhënave personale;
- qëllime të përpunimit;
- përshkrim të kategorive të subjektit të të dhënave personale dhe kategoritë e të dhënave personale;
- kategoritë e shfrytëzuesve të të dhënave personale të cilëve u janë zbuluar ose do t'u zbulohen të dhënat personale, duke përfshirë edhe shfrytëzues të vendeve të treta ose organizata ndërkombëtare;
- bartja e të dhënave personale në vende të treta ose organizata ndërkombëtare, duke përfshirë edhe dokumentacion për zbatimin e masave adekuate të sigurisë;
- afate kohore të parapara për fshirje të kategorive të ndryshme të të dhënave personale; dhe
- përshkrim të përgjithshëm të masave të zbatuara teknike dhe organizative.

Gjithashtu, çdo përpunues është përgjegjës dhe mban evidencë për të gjitha kategoritë e aktiviteteve për përpunim që i kryen në emër të kontrolluesit me informacionet si vijojnë

- emër dhe kontakt të detajuar të përpunuesit/përpunuesit dhe çdo kontrollues në emër të secilit vepron përpunuesi dhe oficeri për mbrojtjen e të dhënave personale, kur ajo është e zbatueshme;
- kategoritë e të dhënave personale që përpunohen në emër të çdo kontrolluesi;
- bartja e të dhënave personale në vende të treta ose organizatë ndërkombëtare, duke përfshirë edhe dokumentacionin për zbatimin e masave përkatëse të sigurisë;
- përshkim të përgjithshëm të masave të zbatuara teknike dhe organizative.

Institucionet financiare me më pak se 50 të punësuar janë përjashtuar nga detyrimi për mbajtjen e evidencës, përveç nëse është e besueshme se përpunimi që kryhet paraqet rrezik për rregullat dhe liritë e subjekteve të të dhënave personale, nëse përpunuesi përpunon kategori të posaçme të të dhënave personale dhe nëse përpunimi nuk kryhet vetëm përkohësisht. Në praktikë, ky përjashtim rrallë mund të zbatohet. Përveç pengesave që paraqiten në lidhje me interpretimin që nënkuptohet " vetëm përkohësisht", në rast të numrit të madh të institucioneve financiare të pakontestueshme është se ato rregullisht përpunojnë të dhëna personale, duke përfshirë edhe përpunim të të dhënave personale për ueb faqet e tyre, për banking elektronik, ejt., edhe me zbatim të interpretimit të gjerë për termin të dhëna.

Duhet të theksohet se obligimi për dokumentim dhe, bazuar në këtë, evidenca e aktiviteteve për përpunim do të jetë në fokus të supervizionit që e zbaton AMDHP.

9. SIGURIA E TË DHËNAVE PERSONALE

Zbatimi i masave përkatëse organizative dhe teknike që të sigurohet nivel i caktuar i sigurisë kundrejt rrezikut ka rol kryesor në arritjen e harmonizimit nga ana e institucioneve në sektorin financiar.

Neni 36 nga LMDHP-ja përcakton disa nga masat që mund t'i zbatojnë kontrolluesit siç janë:

a. psedumonimizimi dhe kripitimi i të dhënave personale;
b. aftësia për sigurimin e besueshmërisë së vazhdueshme, integritet, qasjes dhe rezistencës së sistemit dhe shërbimeve të përpunimit;
c. aftësia për vendosje në kohë, rivendosje të arritjes së të dhënave personale dhe qasje deri te ato në rast të incidenteve fizike ose teknike;
d. procesi për testim të rregullt, vlerësimi dhe evaluimi i efektivitetit të masave teknike dhe organizative që të garantohet siguria e përpunimit.

Në pajtim me nenin 66, paragrafin (6) nga LMDHP, AMDHP ka miratuar dhe publikuar Rregullore për siguri të përpunimit të të dhënave personale e cila jep udhëzime për aktivitet që kontrolluesit duhet t'i ndërmarrin në lidhje me zbatimin e masave teknike dhe organizative për siguri të të dhënave personale. Rregullorja është e arritshme në linkun si vijon.

Përveç kësaj siguria e përpunimit të të dhënave personale është theksuar në mënyrë plotësuese nëpërmjet obligimit të kontrolluesve dhe përpunuesve për t'i paraqitur incidentet (cenimet e sigurisë së të dhënave personale) deri te AMDHP, kurse në disa raste edhe deri te subjekti i të dhënave personale (neni 37 dhe 38 nga LMDHP).

Sipas LMDHP dhe në pajtim me parimet e mirënjohura për siguri informatike, cenimi i sigurisë së të dhënave personale mund të grupohet në kategoritë si vijojnë: "cenimi i besueshmërisë"- zbulim ose qasje e paautorizuar ose e rastësishme te të dhënat personale; "cenimi i integritetit"- ndërrim i paautorizuar ose i rastësishëm i të dhënave personale; " cenimi i arritshmërisë"- humbje e paautorizuar ose e rastësishme e qasjes te ose asgjësimi i të dhënave personale.

Mund të thuhet se pjesëmarrësit nga sektori financiar përpunojnë sasi të mëdha të të dhënave që mund të konsiderohen të dhëna të ndjeshme (sepse shkelja e lidhur me këto të dhëna ka ndikim serioz mbi jetën e përditshme të subjektit të prekur të të dhënave personale, për shembull, të dhëna financiare të cilat mund të shfrytëzohen për pagim mashtrues), që e rrit rrezikun potencial.

Duke pasur parasysh se baza e Ligjit për të dhëna personale paraqet qasje që bazohet në rrezik, institucionet nga industria financiare duhet të zbatojnë vlerësime periodike të rrezikut, të zhvillojnë politika të brendshme dhe procedura për ndjekje efektive, reagimin dhe zbutjen e pasojave nga incidente potenciale të sigurisë. Një nga detyrimet më të rëndësishme të kontrolluesit është vlerësimi i rreziqeve për të drejtat dhe liritë e subjektit të të dhënave personale dhe marrjen e teknikave adekuate dhe masave organizative për zgjedhjen e të njëjtave.

9.1. Njoftim për prishjen e sigurisë së të dhënave personale

LMDHP vendos detyrim sipas të cilit prishja e sigurisë së të dhënave personale duhet të paraqitet në AMDHP (neni 37) dhe, në disa raste, për prishjet duhet të informohen

Trajnimi dhe ndërtimi i vetëdijes për çështjet lidhur me mbrojtjen e të dhënave personale te personeli i kontolluesit në fokus të menaxhimit me prishjen e sigurisë së të dhënave personale janë me rëndësi esenciale për kontrolluesit në kuadër të aktiviteteve të tyre lidhur me masat për sigurimin e nivelit adekuat të sigurisë.

personat të cilët janë të prekur personalisht nga cenimi i atyre të dhënave (neni 38).

Detyrimi i ri për njoftim sjell numër të madh të përfitimeve. Nëpërmjet njoftimeve të Agjencisë, kontrolluesit mund të marrin këshilla për atë nëse subjektet e prekura nga të dhënat personale duhet të jenë të informuar ose mund të marrin urdhër t'i informojnë personat për cenimin. Informimi i personave fizikë për cenim të sigurisë së të dhënave personale i lejon kontrolluesit të japin informacione për rreziqet që janë rezultat i cenimit të tillë dhe për hapat që personat e prekur mund të ndërmarrin që të mbrohen nga pasojat potenciale.

Në nenin 4, pika 12), ligji e definon "cenimin e sigurisë së të dhënave personale" si cenim të sigurisë që çon deri në asgjësimin, ndryshimin e rastësishëm dhe të paligjshëm, zbulimin e paautorizuar ose qasje deri te të dhënat personale që transmetohen, ruhen ose përpunohen në mënyrë tjetër.

Shembull për humbjen e të dhënave personale përfshin edhe vjedhja e pajisjes që përmban kopje nga baza e të dhënave personale me klientët e kontrolluesit

Shembull për humbjen e qasjes deri te të dhënat personale përfshijnë shlyerje të rastësishme ose shlyerje të të dhënave personale nga ana e personi të paautorizuar, ose humbjen e çelësit për dekriptim kur bëhet fjalë për të dhëna të kriptuara

Ligji imponon edhe kontrolluesit edhe përpunuesit të zbatojnë masa adekuate teknike dhe organizative që duhet të sigurojnë nivel të mbrojtjes që është adekuat me rrezikun për të dhënat personale që përpunohen. Nga këtu, masat adekuate teknike dhe organizative duhet menjëherë të jenë shembull pa marrë parasysh nëse ka ndodhur cenimi i sigurisë së të dhënave personale, që më vonë përcakton nëse aktivizohet obligimi për njoftim. Si rezyme, element kryesor i çdo politike për siguri të të dhënave personale është aftësia, kur ajo është e mundshme, të pengohet cenimi dhe në rast të cenimit, është e rëndësishme të merret reagim në kohë.

10. VLERËSIMI I NDIKIMIT MBI MJEDISIN JETËSOR TË TË DHËNAVE PERSONALE DHE KONSULTIMEVE PARAPRAKE

LMDHP imponon kontrolluesit të zbatojnë masa adekuate që të sigurojnë dhe të jenë në mundësi të demonstrojnë harmonizim me ligjin nëpërmjet shqyrtimit të, mes tjerash, rreziqeve nga besueshmëri të ndryshme dhe seriozitetit për të drejtat dhe liritë e personave fizikë (neni 28, paragrafi (1) nga LMDHP).

Vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale (VNMDHP) është proces i cili është dizajnuar ta përshkruajë përpunimin, ta vlerësojë domosdoshmërinë dhe proporcionalitetin e tij, dhe t'i ndihmojë në menaxhimin me rreziqe për të drejtat dhe liritë e personave fizikë në lidhje me përpunimin e të dhënave personale nëpërmjet vlerësimit dhe përcaktimit të masave për zgjedhjen e tyre.

VNMDHP është mjet i rëndësishëm i llogaridhënies sepse ajo mund tu ndihmojë kontrolluesve jo vetëm të harmonizohen me kërkesat nga LMDHP, por edhe të demonstrojnë se janë zbatuar masa adekuate.

Sipas qasjes që bazohet në rrezik, zbatimi i vlerësimit të ndikimit nuk është i detyrueshëm për çdo operacion për përpunim që e kryen kontrolluesi. Neni 39, paragrafi (1) nga LMDHP përcakton se vlerësimi i tillë është i nevojshëm kur " ekziston mundësia se përpunimi do të rezultojë me rrezik të lartë për të drejtat dhe liritë e personit fizik".

Lloj i tillë i operacioneve për përpunim mund të jenë operacionet të cilat nënkuptojnë shfrytëzimin e teknologjive të reja ose nënkuptojnë operacione për përpunim voluminoz me qëllim të përpunohet vëllim i konsiderueshëm i të dhënave personale në nivel rajonal ose nacioanal, kurse të cilat mund të ndikojnë mbi numër të madh të subjekteve të të dhënave personale dhe për të cilat ekziston besueshmëri se do të rrezultojë me rrezik të lartë, për shembull, kur të dhënat personale përpunohen për miratimin e vendimeve për persona fizikë konkret sipas ndonjë lloji të evolucioni sistematik dhe ekstenziv të veçorive personale të personave në lidhje me plotësimin e kritereve për kredibilitet ose kushtet që i ofrojnë kreditorët.

LMDHP përcakton se VNMDHP duhet të zbatohet në rastet si vijojnë:

(a) vlerësim gjithëpërfshirës dhe sistematik i aspekteve personale që janë lidhur me personat fizikë, i cili bazohet në përpunimin automatik, duke përfshirë edhe profilim, kurse në bazë të të cilit miratohen vendimet që prodhojnë veprim juridik në lidhje me personin fizik ose ndikojnë në personin fizik;

(b)përpunim voluminoz i kategorive të posaçme të të dhënave personale nga neni 13, paragrafi (1) nga LMDHP, ose të dhëna personale lidhur me dënime penale dhe vepra penale nga neni 14 nga LMDHP; ose

(v) mbikëqyrje sistematike e hapësirave publikisht të arritshme me përmasa më të mëdha.

Në mënyrë plotësuese, duhet të vërehet se AMDHP ka miratuar dhe publikuar disa dokumente në këtë fushë, respektivisht:

Rregullore për procesin e vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale

Lista e llojeve të operacioneve për përpunim të cilat nuk imponojnë vlerësim të ndikimit mbi mbrojtjen e të dhënave personale

Lista e llojeve të operacioneve për përpunim të cilat imponojnë vlerësim të ndikimit mbi mbrojtjen e të dhënave personale

Nëse kontrolluesi, si pjesë e vlerësimit të tij, ka përfunduar se rreziqet duhet të konsiderohen mjaftueshëm të zvogëluara, në pajtim me dispozitat e nenit 40, paragrafit (1) nga LMDHP, përpunimi mund të vazhdojë pa konsultim me AMDHP. Në rastet kur rreziqet e identifikuara nuk mund të jenë mjaftueshëm të liruara nga ana e kontrolluesit dhe kur kontrolluesi nuk mund të gjejë masa të mjaftueshme për uljen e rreziqeve deri në nivel të pranueshëm, atëherë duhet të organizohen konsultime me AMDHP.

Në pajtim me dispozitat nga neni 39, paragrafi (1) nga LMDHP, kontrolluesi është ai i cili zbaton vlerësim të ndikimit mbi mbrojtjen e të dhënave personale. Megjithatë, oficeri për mbrojtjen e të dhënave personale mund të ketë rol shumë të rëndësishëm dhe të favorshëm nëpërmjet dhënies së ndihmës kontrolluesit. Për këtë qëllim, neni 39, paragrafi (2) konkretisht imponon kontrolluesi të kërkojë këshillë nga oficeri për mbrojtjen e të dhënave personale gjatë zbatimit të vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale. Më tej, neni 43 paragrafi (1), alineja v) nga LMDHP përcakton se detyrat e oficerit për mbrojtjen e të dhënave personale përfshin dhënien e këshillave për vlerësim të ndikimit dhe ndjekjen e zbatimit të vlerësimit të tillë sipas nenit 39 nga LMDHP.

11. OFICERI PËR MBROJTJEN E TË DHËNAVE PERSONALE

Sipas dispozitave nga neni 41, paragrafi (1) nga LMDHP, kontrollues dhe përpunues të caktuar janë të detyruar të caktojnë oficer për mbrojtjen e të dhënave personale. Më konkretisht, ligji imponon përcaktimin e oficerit të tillë në tre raste konkrete:

a. përpunimi kryhet nga organi i administratës shtetërore, përveç për gjykatat kur veprojnë në kuadër të kompetencave të tyre, ndërsa të cilët caktojnë oficer për përpunimin tjetër të të dhënave personale në pajtim me ligjin
b. aktivitetet themelore të kontrolluesit ose përpunuesit përbëhen nga operacionet e përpunimit, të cilat për shkak të natyrës, fushëveprimit dhe/ose qëllimeve, në masë të madhe imponojnë ndjekjen e rregullt dhe sistematike të subjekteve të të dhënave personale; ose
c. aktivitetet themelore të kontrolluesit ose përpunuesit përbëhen nga përpunimi i gjerë i kategorive të veçanta të të dhënave personale ose të të dhënave personale në lidhje me dënimet penale dhe veprat penale nga neni 14 i këtij ligji.

Në lidhje me institucionet financiare, neni i lartpërmendur 41 paragrafi (1), pika b) nga LMDHP udhëzojnë në aktivitete bazë të kontrolluesit ose përpunuesit. Koncepti

"aktivitete bazë" nuk duhet të interpretohet se përjashton aktivitete ku përpunimi i të dhënave personale është pjesë e pandashme nga veprimtaria e kontrolluesit ose e përpunuesit. Për shembull, sipas nenit 2 pika (2) nga Ligji për bankat (" Gazeta Zyrtare e RM-së" numër 67/2007, 90/2009, 67/2010, 26/2013, 15/2015, 153/2015, 190/2016, 7/2019, 101/2019 dhe 122/2021), " aktivitete bankare" me grumbullimin e depozitave dhe miratimin e kredisë në emër të tij dhe për llogari të tij; kurse sipas nenit 4, paragrafi (1) dhe (2) nga Ligji për shoqëri financiare (" Gazeta Zyrtare e RM-së" numër 158/2010, 169/2010, 53/2011, 112/2014, 153/2015 dhe 23/2016), një shoqëri financiare mund të kryejë një ose më shumë nga aktivitetet në vijim: miratimin e kredive, dhe lëshimin dhe administrimin e kartelave kreditore.

Duke pasur parasysh se një bankë ose institucion financiar nuk mund t'i kryejë aktivitetet e tyre pa përpunim të të dhënave personale të klientit, përpunimi i këtyre të dhënave duhet të llogaritet si një nga aktivitetet bazë të bankës ose institucionit financiar.

Më tej, dispozitat e cituara ligjore imponojnë përpunim të vëllimshëm të të dhënave personale, por nuk definojnë çka paraqet "përpunimi vëllimor". Edhe pse nuk mund të jepet numër preciz në raport të vëllimit të të dhënave të përpunuara ose numrin e personave të cilët janë prekur nga situata konkrete, nuk përjashtohet mundësia për zhvillim të praktikave standarde me qëllim më saktë të përgjigjet në pyetjen për atë që paraqet "përpunimi voluminoz", në raport të llojeve të caktuara të aktiviteteve për përpunim.

Për këtë qëllim, duhet të merren parasysh faktorët si vijojnë: numri i subjekteve të prekura të të dhënave personale, vëllimi i të dhënave të cilat përpunohen, kohëzgjatja e aktivitetit për përpunim, përfshirja gjeografike e aktivitetet për përpunim. Nga këtu, për shembull, përpunimi i të dhënave të klientëve si aktivitet i rregullt afarist në një bankë mund të konsiderohet si përpunim i "vëllimshëm".

Ku bëhet fjlë për pozitën e oficerit për mbrojtjen e të dhënave personale, neni 42 nga LMDHP përcakton se kontrolluesi dhe përpunuesi siguron përfshirje të oficerit, në mënyrë edukate dhe në kohë, në të gjitha çështjet të cilat kanë të bëjnë me mbrojtjen e të dhënave personale nëpërmjet sigurimit të përkrahjes për kryerjen e detyrave të tij nga neni 43 nga LMDHP. Për atë qëllim, neni 42, paragrafi (6) nga LMDHP përcakton se oficeri për mbrojtjen e të dhënave personale, mund të kryejë edhe detyra dhe obligime tjera jashtë nga ato të specifikuara me këtë ligj, por kontrolluesi ose përpunuesi është i detyruar të sigurojë se detyrat dhe ngarkimet e tilla nuk do të shkaktojnë konflikt të interesave, që është e lidhur me kërkesën e oficerit për të vepruar në mënyrë të pavarur. Me fjalë të tjera, oficeri nuk mund ta kryejë pozicionin në kuadër të organizatës e cila nënkupton përcaktimin e qëllimit dhe mjetet për përpunimin e të dhënave personale. Pozicionet e tilla në kuadër të organizatës mund të jenë: drejtor kryesor financiar, udhëheqës i seksionit për resurse njerëzore ose udhëheqës i seksionit për teknologji informatike.

Në fund, duhet të theksohet se oficerët për mbrojtjen e të dhënave personale nuk janë personalisht përgjegjës në rast të mosharmonizimit me LMDHP. LMDHP udhëzon qartë për atë se kontrolluesi dhe përpunuesi janë ata të cilët duhet të sigurojnë dispozitat dhe të jenë në mundësi të demonstrojnë se përpunimi kryhet në pajtim me dispozitat e nenit 28, paragrafit (1). Nga këtu, harmonizimi me mbrojtjen e të dhënave personale është përgjegjësi e kontrolluesit ose përpunuesit.

12. BARTJA E TË DHËNAVE PERSONALE JASHTË TERRITORIT TË REPUBLIKËS SË MAQEDONISË Ë VERIUT

Korniza juridike për mbrojtjen e të dhënave personale në Republikën e Maqedonisë së Veriut e pranon vlefshmërinë e rrezikut të rritur për të dhënat personale në lidhje me bartjen e të dhënave në vende të treta ose organizata ndërkombëtare dhe prandaj përmban kërkesa konkrete të cilat kanë për qëllim të ofrojnë nivel të njëjtë të mbrojtjes edhe për të dhënat të cilat barten jashtë territorit të Republikës së Maqedonisë së Veriut.

Në mënyrë plotësuese në harmonizimin me kushtet e përcaktuara në dispozitat tjera nga ligji, subjektet që kryejnë bartjen e të dhënave personale në vende të treta ose organizata ndërkombëtare duhet të sigurohen, në bazë të nga-rasti në rast, se masat e parapara për bartjen e të dhënave personale në vende të treta janë qartë të zbatueshme edhe të instrumentit për bartje.

Në përgjithësi, gjatë zbatimit të dispozitave për bartjen e të dhënave personale, kontrolluesit dhe përpunuesit duhet të zbatojnë qasje me më shumë shtresa, respektivisht:

- së pari, ata duhet të shqyrtojnë nëse vendi i tretë siguron nivel adekuat të mbrojtjes, respektivisht nëse Agjencia për Mbrojtjen e të Dhënave Personale (AMDHP) ka marrë vendim në pajtim me dispozitat nga neni 49 nga LMDHP se vendi i tretë konkret ose organizata ndërkombëtare siguron nivel adekuat të mbrojtjes.
- e dyta, nëse ekziston vendim për nivel adekuat për mbrojtje në rastin konkret, subjekti që kryen bartje të të dhënave personale duhet të mendojë për zbatim të masave adekuate të sigurisë dhe bartjen ta vendosë në një nga mekanizmat e dhënë në nenin 50 nga LMDHP;
- vetëm në mungesë të instrumentit të arsyetuar në zërat paraprakë, kontrolluesi ose përpunuesi mund të bazohet në shmangiet e dhëna në nenin 53 nga LMDHP.

Kur flasim për llojet e shmangies, duhet të shënohet se ato duhet të interpretohen me vëmendje, në mënyrë të kufizuar dhe vetëm në bazë nga rasti-në rast. Për shembull, baza juridike "interes i rëndësishëm publik" nënkupton interes i cili është identifikuar si i i tillë në legjislacionin nacional që ka të bëjë në kontrolluesit e vendosur në Republikën e Maqedonisë së Veriut.

Në lidhje me shërbimet financiare, masa të caktuara i mundësojnë kontrolluesit të shkojnë më larg nga detyrimet e tyre konkrete ligjore gjatë zbatimit të ligjeve për luftë kundër aktiviteteve të paligjshme, siç është larja e parave ose zbulimi i mashtrimeve. Nëse konsiderohet se ajo është interes i rëndësishëm publik sipas ligjeve nacionale të cilat zbatohen për kontrolluesin, atëherë kjo shmangie mund të zbatohet në bartjen e të dhënave personale deri te organet kompetente në vende të treta. Megjithatë, interesi publik nuk mund të shfrytëzohet për arsyetim të bartjes së sërishme, të vëllimshme ose strukturore të cilat kanë të bëjnë me transmetim të madh të propozuar të të dhënave personale deri te vende të treta për parandalimin të larjes së parave.

Nëse asnjë nga shmangiet nuk është e zbatueshme, atëherë subjekti që kryen bartje të të dhënave personale duhet të zbatojë masa të sigurisë adekuate që të sigurojë se subjektet e atyre të dhënave janë të mbrojtura në mënyrë adekuate nëpërmjet instrumenteve obligative dhe ligjore . Në rast të subjekteve private, ajo zakonisht ka formë të marrëveshjes së shkruar në të cilën janë inkorporuar klauzolat e marrëveshjeve standarde, rregullat e detyrueshme korporative ose lloj tjetër i marrëveshjeve ad-hok mes subjektit që kryen transmetim dhe subjektit që pranon të dhëna në vende të treta.

Për informata më të detajuara në lidhje me bartjen e të dhënave personale jashtë nga territori i Republikës së Maqedonisë së Veriut dhe instrumentet e mundshme për bartje shihni Udhëzuesin për bartjen e të dhënave personale në vende të treta dhe organizata ndërkombëtare të publikuara në ueb faqen e AMDHP-së.

Projekt – twining i BE-së „Mbështetje në zbatimin e kornizës së modernizuar ligjore për mbrojtjen e të dhënave personale”

Ky publikim është prodhuar me ndihmën financiare të Bashkimit Evropian. Përmbajtja e këtij publikimi është përgjegjësi vetëm e autorit dhe në asnjë mënyrë nuk mund të konsiderohet se pasqyron pikëpamjet e Bashkimit Evropian.

Kërkoni më shumë informacione në
www.azlp.mk

SCAN ME

Ky projekt financohet nga Bashkimi Evropian