UDHËZUES PËR NJOFTIME PËR

CENIMIN E SIGURISË SË TË DHËNAVE PERSONALE

Ky projekt financohet nga Bashkimi Evropian

PËRMBAJTJA

HYRJE

Ligji për mbrojtjen e të dhënave personale (në tekstin e më poshtëm: LMDHP) vendos detyrim për njoftim të Agjencisë për Mbrojtjen e të Dhënave Personale (organ mbikëqyrës nacional) për cenimin e sigurisë së të dhënave personale dhe, në disa raste, detyrimi për informim të personave fizikë kur ata janë të prekur nga cenimi konkret.

LMDHP përcakton se njoftimet janë të detyrueshme për të gjithë kontrolluesit, përveç nëse nuk ekziston besueshmëri se cenimi i sigurisë së të dhënave personale do të rezultojë në rrezik të lartë për të drejtat dhe liritë e personave fizikë. Përpunuesit kanë rol të rëndësishëm në këtë procedurë sepse duhet ta njoftojnë kontrolluesin për të gjitha cenimet e sigurisë së të dhënave personale.

Detyrimi për njoftim bart numër të madh të përftimeve. Kur e informon AMDHP, kontrolluesit mund të marrin këshilla nëse personat fizikë të prekur duhet të jenë të informuar. Në rast të tillë AMDHP mund t'i urdhërojë kontrolluesit t'i informojnë palët e prekura për cenimin e sigurisë së të dhënave personale. Nga ana tjetër, informimi i personave fizikë për ngjarje të tillë u mundëson kontrolluesve të sigurojnë informacione për rreziqet të cilat rezultojnë nga cenimi i sigurisë së të dhënave personale dhe për hapat që personat e prekur mund t'i ndërmarrin që të mbrohen nga pasojat e mundshme. Planet për ballafaqim me cenimin e sigurisë së të dhënave personale duhet të fokusohen në mbrojtjen e personave fizikë dhe të të dhënave personale. Rrjedhimisht, njoftimi për cenimin e sigurisë së të dhënave personale konsiderohet mjet i rëndësishëm i cili e forcon harmonizimin e dispozitave për mbrojtjen e të dhënave personale. Në të njëjtën kohë duhet të vërehet se mosparaqitja e njoftimit te personat fizikë ose te AMDHP tërheq shqiptimin e sanksioneve për kontrolluesin dhe/ose përpunuesin, në pajtim me nenin 110 paragrafin (1) pikën 11) dhe 12) nga LMDHP.

Prandaj kontrolluesit dhe përpunuesit inkurajohen të përgatisin plane dhe të vendosin procedura që do t'i mundësojë identifikim në kohë dhe ndërprerje të cenimit të sigurisë së të dhënave personale, t'i vlerësojnë rreziqet për personat fizikë dhe më pas të përcaktojnë nëse është e nevojshme të dorëzojnë njoftim te AMDHP dhe të informohen personat fizikë të cilët janë prekur me cenimin. Njoftimi te AMDHP duhet të jetë pjesë nga plani i tillë për ballafaqim me incidente.

LMDHP përmban dispozita të cilat rregullojnë kur dhe kush duhet të njoftohet për cenimin e sigurisë së të dhënave personale, si dhe llojin e informacioneve që duhet të jepen si pjesë nga njoftimi. Informacionet nga njoftimi mund të sigurohen gradualisht (në faza), por në të gjitha rastet kur kontrolluesi duhet të reagojnë në kohë për çdo cenim të sigurisë.

1. NJOFTIM PËR CENIMIN E SIGURISË SË TË DHËNAVE PERSONALE SIPAS LMDHP

1.1. Vërejtje të përgjithshme për sigurinë

Një nga kushtet që i përcakton LMDHP ka të bëjë me zbatimin e masave adekuate organizative dhe teknike që të sigurohet se të dhënat personale përpunohen në mënyrë që përfshin mbrojtjen e të dhënave personale, respektivisht mbrojtjen nga përpunimi i paautorizuar ose joligjor dhe nga humbja e rastësishme, asgjësimin ose dëmtimin e të dhënave.

Rrjedhimisht, LMDHP u imponon kontrolluesve dhe përpunuesve të zbatojnë masa adekuate teknike dhe organizative që të sigurojnë nivel të sigurisë që përgjigjet me rrezikun nga përpunimi i të dhënave personale. Ata duhet t'i marrin parasysh teknologjitë më të reja, shpenzimet për zbatim, si dhe natyrën, vëllimin, kontekstin e qëllimeve të përpunimit, dhe rreziqet me mundësi të ndryshme dhe seriozitet për të drejtat dhe liritë e personave fizikë.

Nga këtu element kryesor për çdo politikë të sigurisë së të dhënave personale është kontrolluesi të jetë i përgatitur, kur ajo është e mundshme, ta ndërpresë cenimin e sigurisë së të dhënave personale, ndërsa kur kjo megjithatë do të ndodhë, do të reagojë në kohë.

1.2. Çka është cenim i sigurisë së të dhënave personale

1.2.1. Definicioni

Si pjesë e tentativës për zgjedhjen e cenimit të sigurisë së të dhënave personale, kontrolluesit së pari duhet të jetë në mundësi të njohin se bëhet fjalë për ngjarje të tillë. Në nenin 4, pika 12), LMDHP e jep definicionin si vijon " cenimi i sigurisë së të dhënave personale":

"çdo cenimi i sigurisë që rastësisht çon në asgjësim të paligjshëm, humbje, ndryshim, zbulim të paautorizuar ose qasje te të dhënat personale që transmetohen, ruhen ose përpunohen në mënyrë tjetër".

Kjo që nënkuptohet me "asgjësim" të të dhënave personale duhet të jetë mjaftë e qartë: ai është momenti kur të dhënat më nuk ekzistojnë ose nuk ekzistojnë në format në të cilat i shfrytëzon kontrolluesi". Dhe "ndryshimi" i të dhënave personale është relativisht evident: ai është momenti kur të dhënat personale janë ndryshuar, korruptuar ose më nuk konsiderohen të plota. "Humbja" e të dhënave personale duhet të interpretohet si ekzistim i mundshëm i të dhënave, por kontrolluesi ka humbur kontroll mbi ose qasje te ato, ose të dhënat më nuk janë në pronësi të tij. Në fund, "përpunimi i paautorizuar ose jo ligjor" mund të përfshijë zbulim të të dhënave personale (ose dhënien e qasjes te të dhënat) të shfrytëzuesve të cilët nuk janë të autorizuar për marrje ose qasje te të

dhënat, ose në ndonjë formë tjetër të përpunimit e cila është në kundërshtim me LMDHP.

Shembull:
Shembull për humbjen e të dhënave personale mund të jetë situata në të cilën pajisja që përmban kopje nga baza e klientëve të kontrolluesit është vjedhur ose humbur. Shembull tjetër për humbje të të dhënave personale mund të jetë situata në të cilën kopja e vetme nga të dhënat personale është kriptuar nga haker me ransomver (softuer malicioz) ose ajo është kriptuar nga kontrolluesi me çelës i cili më nuk është në pronësi të tij.

Ajo që duhet të jetë e qartë se cenimi është lloj i incidentit të sigurisë. Megjithatë, në pajtim me definicionin nga neni 4, pika 12) nga LMDHP, dispozitat e ligjit zbatohen vetëm në rast të cenimit të sigurisë së të *dhënave personale.* Pasojat për kontrolluesit nga cenimi i tillë përfshijnë mosharmonizim me parimet për përpunimin e të dhënave personale, ashtu siç janë dhënë në nenin 9 nga LMDHP. Ai e thekson dallimin mes incident sigurie dhe cenimin e sigurisë së të dhënave, përkatësisht edhe pse të gjitha cenimet konsiderohen për incidente sigurie, por jo të gjitha incidentet e sigurisë detyrimisht përfshijnë cenim të sigurisë së të dhënave personale.

1.2.2. Llojet e cenimit të sigurisë së të dhënave personale

Cenimi mund të karakterizohet sipas tre parimeve mirë të njohura për siguri informatike:

- "cenimi i besueshmërisë"- kur ekziston zbulim i paautorizuar ose zbulim i rastësishëm ose qasje te të dhënat personale;
- "cenim i integritetit"- kur ekziston ndërrim i autorizuar ose i rastësishëm i të dhënave personale;
- "cenimi i qasshmërisë"- kur ekziston humbje e paautorizuar ose e rastësishme e qasjes te ose shkatërrimi i të dhënave personale.

Duhet të shënohet se, në varësi të rrethanave, cenimi i sigurisë së të dhënave personale njëkohësisht mund të ketë të bëjë me besueshmërinë, integritetin dhe qasjen e të dhënave personale, ose mund të ketë të bëjë me cilin do kombinim nga këto tri situata.

Nëse konstatimi i faktit nëse bëhet fjalë për cenim të besueshmërisë ose cenim të integritetit është relativisht i thjeshtë, konstatimi nëse ekziston cenim i arritshmërisë së të dhënave personale nuk do të jetë aq evident. Humbja permanente ose asgjësimi i të dhënave personale çdo herë konsiderohet cenim i arritshmërisë së të dhënave personale.

Shembuj për mos qasje të të dhënave personale përfshijnë situata në të cilat të dhënat janë shlyer rastësisht ose zgjedhur nga ana e personit të paautorizuar, ose kur është humbur çelësi për dekriptim të të dhënave personale të cilat janë kriptuar paraprakisht

nga arsye të sigurisë. Kur kontrolluesi nuk mund ta kthejë qasjen te të dhënat, për shembull, nga kopja rezervë e të dhënave, ajo konsiderohet humbje e përhershme e arritshmërisë. Mos arritshmëria e të dhënave personale mund të paraqitet edhe kur ka cenim të konsiderueshëm të punës normale të një organizate, për shembull, nëse ajo ballafaqohet me ndërprerje të energjisë elektrike ose me sulm për refuzim të shërbimit (denial of service), me ç'rast të dhënat bëhen më të pa arritshme.

Këtu parashtrohet pyetja nëse mos qasja e përkohshme tek të dhënat personale duhet të konsiderohet si cenim i sigurisë dhe kush duhet të jetë i njoftuar për të njëjtën. Neni 36 nga LMDHP ka të bëjë në sigurinë e përpunimit të të dhënave personale dhe përcakton se kur zbatojë masa teknike dhe organizative për sigurimin e nivelit adekuat të sigurisë që përgjigjet me rrezikun, mes tjerash, kontrolluesit duhet të tregojnë " aftësi për sigurimin e besueshmërisë të vazhdueshme, integritet, arritshmëri dhe rezistencë të sistemit dhe shërbimet për përpunim" dhe " aftësi për kthim në kohë të arritshmërisë dhe qasje te të dhënat personale në rast të incidentit teknik ose fizik.

Nga këtu mund të konkludohet se incident i sigurisë i cili rezulton në mos arritshmëri të të dhënave personale në periudhë të caktuar kohore është lloj i cenimit të sigurisë së të dhënave personale sepse pamundësia të qaset te të dhënat mund të ketë ndikim të konsiderueshëm mbi të drejtat dhe liritë e personave fizik. Megjithatë , situata në të cilën të dhënat personale janë të paarritshme për shkak të mirëmbajtjes së planifikuar të sistemit nuk konsiderohet për cenim të sigurisë së të dhënave personale sipas definicionit të dhënë në nenin 4, pika 12) nga LMDHP.

Gjithashtu situata me humbje ose shkatërrim të të dhënave personale (ose çfarë do lloji tjetër të cenimi të sigurisë së të dhënave personale), cenimi i cili nënkupton mos qasje të përkohshme të të dhënave personale duhet të jenë të dokumentuar në pajtim me nenin 37 paragrafi (5) nga LMDHP./ Ajo i ndihmon kontrolluesve të tregojnë llogaridhënie para AMDHP, e cili mund t'i kërkojë shkresat e tilla. Në varshmëri të rrethanave, cenimi i sigurisë së të dhënave personale mund, por jo domosdoshmërish, të impojnë detyrim për njoftim të AMDHP dhe informimin e personave fizikë të prekur. Kontrolluesi duhet ta vlerësojnë probabilitetin dhe seriozitetin e ndikimit nga mos arritshmëria e të dhënave personale mbi të drejtat dhe liritë e personave fizik. Sipas nenit 38 nga LMDHP, kontrolluesit duhet t'i informojnë subjektet e të dhënave personale përveç nëse nuk ekziston probabilitet se cenimi do të rezultojë në rrezik për të drejtat dhe liritë e tyre. Nënkuptohet, vlerësim i tillë bohet në bazë individuale për çdo rast individualisht.

Shembuj:
Nëse të dhënat mjekësore kritike për pacientët e një spitali janë të paarritshme, edhe përkohësisht, ajo mund të paraqesë rrezik për të drejtat dhe liritë e personave fizik, për shembull, anulimin e operacionit kirurgjik dhe vënia e jetës në rrezik.

Në rast të paarritshmërisë të sistemit të një shtëpie mediatike në periudhë prej disa orëve (për shembull, për shkak të ndërprerjes së energjisë elektrike), që e pengon

kompania të dërgojë informatorë te parapaguesit, nuk ekziston besueshmëri se ajo do të shkaktojë rrezik për të drejtat dhe liritë e personave fizik.

Duhet të theksohet se edhe paaritshmëria e sistemit të kontrolluesit është e përkohshme dhe ndoshta nuk ndikon mbi personat fizik, është e rëndësishme kontrolluesi t'i shqyrtojë të gjitha pasojat e mundshme nga cenimi i sigurisë së të dhënave personale sepse ajo mund të imponojnë detyrim për njoftim për arsye tjera.

Shembull:
Sulm me ransomver (softuer malicioz që i kripton të dhënat e kontrolluesit deri sa nuk paguhet blerja) mund të sjellë deri në paaritshmëri të përkohshme të të dhënave nëse ato nuk mund të kthehen nga kopja rezervë. Në këtë rast, rrjeti i kontrolluesit është cenuar dhe kjo imponon njoftim nëse incidenti kualifikohet si cenim i besueshmërisë të të dhënave personale (përkatësisht sulmuesi është qasur te të dhënat personale) dhe paraqet rrezik për të drejtat dhe liritë e personave fizik.

1.2.3. Pasojat e mundshme nga cenimi i sigurisë së të dhënave personale

Potencialisht, cenimi i sigurisë së të dhënave personale mund të kenë spektër të gjerë të efekteve negative mbi personat fizik, të cilat mund të rezultojnë në dëm fizik, material dhe jomaterial. Ajo mund të përfshihet në humbje të kontrollit mbi të dhënat e tyre personale, kufizim të të drejtave të tyre, diskriminim, vjedhje të identitetit ose mashtrim identiteti, humbje financiare, kthim i paautorizuar në formë origjinale të të dhënave të pseudonimizuara, autoritet i cenuar dhe humbje e besueshmërisë të të dhënave personale të cilat janë të mbrojtura me fshehtësi afariste. Gjithashtu, ajo mund të përfshijë edhe mos përshtatshmëri të rëndësishme sociale dhe ekonomike për personat e prekur fizik.

Rrjedhimisht, LMDHP i imponon kontrolluesit ta njoftojë AMDHP për cenimin e sigurisë së të dhënave personale, përveç nëse nuk ekziston besueshmëri se ajo do të rezultojë në efekte negative. Kur ekziston probabilitet për rrezik të lartë për paraqitjen e efektive të tilla negative, LMDHP i imponon kontrolluesit t'i informojë personat fizikë të prekur për cenimin e sigurisë së të dhënave personale menjëherë sapo të jetë e realizueshme në mënyrë të arsyeshme.

Nëse kontrolluesi ose përpunuesi nuk e njofton AMDHP ose subjekti i të dhënave personale ose nuk dorëzon asnjë njoftim te asnjë palë edhe krahas faktit se janë plotësuar kushtet nga neni 37 dhe/ose 38 nga LMDH, atëherë AMDHP mund të mendojë për shqiptimin e gjobës kundërvajtëse adekuate në pajtim me nenin 110. Gjatë shqiptimit të gjobës, vlera e saj mund të përcaktohet në shumë prej 2% nga të hyrat e përgjithshme vjetore të kontrolluesit ose përpunuesit - personi juridik (në shumë absolute) të realizuara në vitin afarist që i paraprin vitit kur është kryer kundërvajtja ose nga të hyrat e përgjithshme të realizuara në periudhë prej një vit kur kundërvajtja është kryer nga personi juridik në vitin e parë nga fillimi i punës së tyre.

Duhet të kihet parasysh se, në disa raste, mosparaqitja e njoftimit për cenimin e sigurisë së të dhënave personale mund të drejtohet në mungesë të masave të sigurisë ose masa të sigurisë joadekuate që zbatohen. Disa kundërvajtje të ndryshme të kryera në kohë të njëjtë si pjesë e një rasti do të thotë se organi mbikëqyrës mund të shqiptojë gjobë kundërvajtëse në shumë e cila është efektive, proporcionale dhe ka efekt kthyes, dhe hyn në grupin e kundërvajtjeve më serioze. Në rast të tillë, AMDHP ka mundës të shqiptojë sanksione për mosplotësimin e detyrimit për njoftim të Agjencisë dhe të subjektit të të dhënave personale për cenimin e sigurisë së të dhënave personale (neni 37 dhe 38) nga e njëjta anë, dhe për mosplotësimin e detyrimit për zbatim të masave (adekuate) të sigurisë (neni 36) nga ana tjetër, sepse ato paraqesin kundërvajtje të veçanta.

2. NENI 37: NJOFTIMI I AMDHP

2.1. Kur duhet të paraqitet njoftimi

2.1.1. Kushtet e përcaktuara në nenin 37 nga LMDHP

Neni 37 paragrafi (1) nga LMDHP përcakton se:

"Në rast të cenimit të sigurisë së të dhënave personale, kontrolluesi menjëherë dhe jo më vonë se 72 orë pasi të ka kuptuar për të njëjtën është i detyruar të njoftojë Agjencinë për cenimin e sigurisë së të dhënave personale, përveç nëse nuk ekziston probabilitet që cenimi i sigurisë do të rezultojë me rrezik për të drejtat dhe liritë e individëve. Kur njoftimi në Agjenci nuk është parashtruar në afat prej 72 orëve, bashkë me njoftimin kontrolluesi duhet të dorëzojë edhe arsyetim për shkaqet për vonimin."

2.1.2. Kur kontrolluesi "kupton" për cenimin e sigurisë të të dhënave personale?

Siç ishte theksuar paraprakisht, LMDHP përcakton detyrim se njoftimi për cenimin e sigurisë së të dhënave personale duhet të parashtrohet menjëherë dhe jo më vonë se 72 orë pasi që kontrolluesi ka kuptuar për të njëjtën. Këtu hapet çështja për atë kur konsiderohet se kontrolluesi " ka kuptuar" për cenimin e sigurisë së të dhënave personale. Konsiderohet se kontrolluesi "ka kuptuar" për cenimin e sigurisë kur ekziston nivel i arsyeshëm i sigurisë se ka ndodhur incident i sigurisë i cili ka sjellë deri në kompromet im të të dhënave personale.

Në të njëjtën kohë, LMDHP përcakton edhe detyrimin për kontrolluesit dhe përpunuesit t'i zbatojë të gjitha masat adekuate teknike dhe organizative të të dhënave personale dhe menjëherë ta informojnë AMDHP dhe subjektet e të dhënave personale. Gjatë secilës, gjatë përcaktimit të faktit nëse njoftimi është parashtruar menjëherë dhe pa prolongim të panevojshëm, parasysh duhet të merret natyra dhe serioziteti i cenimit të sigurisë të dhënave personale, si dhe pasojat dhe efektet negative mbi subjektet e të dhënave personale. Nga këtu, kontrolluesi/përpunuesit kanë detyrim të sigurohen se janë në mundësi në kohë të "të kuptojnë" për çdo cenim të sigurisë së të dhënave personale që të mund të ndërmarrin veprime përkatëse.

Kur saktë do të konsiderohet se kontrolluesi " ka kuptuar" për ndonjë cenim të sigurisë së të dhënave personale do varet nga rrethanat në rastin konkret. Në disa raste, ajo do të jetë relativisht e qartë, por edhe në raste tjera është e nevojshme kohë e caktuar të përcaktohet nëse janë kompromet uar të dhënat personale. Megjithatë , theksi vihet në aksion të shpejtë për hulumtim të incidentin që të përcaktohet nëse siguria e të dhënave personale me të vërtetë është cenuar, dhe nëse është ashtu, të ndërmerren veprime konkrete dhe të parashtrohet njoftim, kur ajo është e nevojshme.

Shembuj

1. Në rast kur ndonjë USB pajisje me të dhëna personale të pa kriptuara është humbur shpesh herë nuk munde të konstatohet nëse persona të paautorizuar kanë qasje te të dhënat e pajisjes. Megjithatë , edhe pse kontrolluesi nuk mund të konstatojë nëse ka ndodhur cenim i besueshmërisë e të dhënave personale, situata e tillë duhet të paraqitet sepse ekziston shkallë e arsyeshme e sigurisë se ka ndodhur cenim i besueshmërisë të qasjes të të dhënave personale, por konsiderohet se kontrolluesi " ka kuptuar" për të njëjtën në momentin kur ka kuptuar se USB pajisja ka humbur.

2. Pala e tretë e informon kontrolluesin se ato rastësisht kanë marrë të dhëna personale për një nga klientët e tyre dhe siguron provë për zbulim të paautorizuar të të dhënave personale. Meqë kontrolluesi ka marrë provë të qartë për cenimin e besueshmërisë të të dhënave personale nuk ka dyshim se ai ka "kuptuar" për cenimin.

3. Kontrolluesi zbulon se ekziston ndërhyrje e mundshme në rrjetin e tij. Kontrolluesi i kontrollon sistemet e tyre që të konstatohet nëse të dhënat personale të cilat ruhen në ato sisteme janë kompromet uar dhe vërteton se ajo është ashtu. Sërish, sepse pas kontrollit të zbatuar të kontrolluesit ka provë të qartë për cenimin e sigurisë së të dhënave personale, nuk ka dyshim se ai "ka kuptuar" për ngjarjen.

4. Krimineli kibernetik e kontakton kontrolluesin pasi e ka hakuar sistemin e tij dhe kërkon para që ta ç'kyç. Në rast të tillë, pasi që është bërë kontroll që ta vërtetojë se sistemi është sulmuar, Kontrolluesi ka dëshmi të qartë se ka ndodhur cenim i sigurisë së të dhënave personale dhe nuk ka dyshim se ai ka "kuptuar" për të njëjtën.

Pasi është njoftuar për cenimin potencial të sigurisë të të dhënave personale nga ana e ndonjë personi fizik, mediat ose burim tjetër, ose kur vetë ka zbuluar incident sigurie, kontrolluesit mund t'i duhet periudhë e shkurtë kohore që të hetojë nëse me të vërtetë ka ndodhur cenimi i sigurisë. Nga këtu, derisa zgjat hetimi nuk mund të konsiderohet se kontrolluesi "ka kuptuar" për cenimin. Megjithatë , pritet se hetimi inicial duhet të fillojë sa më shpejtë të jetë e mundur dhe të konstatohet, me nivel të arsyeshëm të sigurisë, nëse me të vërtetë ka ndodhur cenimi i sigurisë së të dhënave personale, me çka mund të bëhet hetim detal.

Pasi ka kuptuar për cenimin e sigurisë së të dhënave personale, kontrolluesi duhet menjëherë dhe më së voni në afat prej 72 orëve të paraqesë njoftim për cenimet të cilat i nënshtrohen detyrimit të tillë. Në atë periudhë kontrolluesi duhet ta vlerësojë probabilitetin e rrezikut për personat fizikë që të konstatohet nëse janë plotësuar kushtet për parashtrim të njoftimit, si dhe veprime që duhet të ndërmerren që të ballafaqohet me cenimin. Kontrolluesi ndoshta veç më ka bërë vlerësim inicial të rrezikut potencial nga cenimi i sigurisë së të dhënave personale si pjesë nga vlerësimi i zbatuar të ndikimit mbi mbrojtjen e të dhënave personale (VNMDHP) para se të fillojë me operacionin për përpunimin e të dhënave personale. Megjithatë , duhet të kihet parasysh se vlerësimi i bërë i ndikimit mund të jetë më i përgjithshëm krahasuar me

rrethanat konkrete të cenimit të sigurisë së të dhënave personale, prandaj kontrolluesi duhet të bëjë vlerësim plotësues dhe t'i marrë parasysh rrethanat konkrete të ngjarjes.

Në më shumë raste, veprimet e tilla preeleminare duhet të mbarohen në periudhë të shkurtë pas alarmit inicial (përkatësisht kur kontrolluesi ose përpunuesi dyshohen se ka ndodhur incident i sigurisë i cili mund të bëjë me të dhënat personale), por në rrethana të jashtëzakonshme ajo mund të zgjatë më gjatë.

Shembull:
Një person e informon kontrolluesin se ka marrë e-postë në të cilën prezantohet si kontrollues dhe e cila përmban të dhëna personale për shfrytëzimin e tij (real) të shfrytëzimin e shërbimeve që i jep kontrolluesi, që udhëzon në faktin se siguria e kontrolluesit është kompromet uar . Kontrolluesi zbaton hetim të shkurtë dhe konstaton ndërhyrje në rrjetin e tij dhe dëshmi për qasje të paautorizuar te të dhënat personale. Në atë moment konsiderohet se kontrolluesi " ka kuptuar" për ngjarjen dhe duhet të paraqesë njoftim te organi mbikëqyrës, përveç nëse nuk ekziston besueshmëri se ajo paraqes rrezik për të drejtat dhe liritë e personave fizikë Në të njëjtën kohë, Kontrolluesi duhet të ndërmarrë masa adekuate kolektive që të ballafaqohet me cenimin e sigurisë së të dhënave personale.

Nga këto arsye, kontrolluesi duhet të ketë vendosur procedura interne të cilat do t'i mundësojnë të zbulojë dhe të ballafaqohet me cenimin e sigurisë së të dhënave personale. Për shembull, që të zbulojë parregullsi në përpunimin e të dhënave personale kontrolluesi ose përpunuesi mund të shfrytëzojë masa të caktuara teknike, siç janë mjete për analizë të lëvizjes të të dhënave personale dhe të shkresave/logeve për qasje te të dhënat, të cilat do të mundësojnë t'i definojnë ngjarjet dhe alarmet përmes zbatimit të të dhënave nga shkresat për qasje. Kur zbulohet cenimi i sigurisë së të dhënave personale, është e rëndësishme të paraqitet te niveli udhëheqës adekuat që të jetë adresuar në mënyrë adekuate dhe që të parashtrojë njoftim, kur ajo është e nevojshme, në pajtim me nenin 37 dhe/ose me nenin 38 nga LMDHP. Masat e tilla dhe mekanizmat për paraqitje duhet të përcaktohen në mënyrë detale në planet për ballafaqim me incidentet dhe/ose aranzhmanet për menaxhim që i ka miratuar kontrolluesi. Ato ndihmojë për planifikim efektiv dhe përcaktim të përgjegjësisë në kuadër të organizatës në lidhje me menaxhimin me cenimin e sigurisë të të dhënave personale, si dhe nëse incidenti mund të eskalojë.

Kontrolluesi duhet të ketë të përcaktuar aranzhman me përpunuesin/përpunuesit të cilët i ka angazhuar dhe të cilët janë të detyruar ta njoftojnë në rast të cenimit të sigurisë së të dhënave personale. Edhe pse kontrolluesit dhe përpunuesit janë përgjegjës për zbatimin e masave adekuate për parandalim, reagim dhe ballafaqim me cenimin e sigurisë së të dhënave personale, më poshtë janë theksuar disa hapa praktik që duhet të ndërmerren në të gjitha rastet:

- Informacionet për të gjitha ngjarjet lidhur me sigurinë dorëzohen te personi / persona përgjegjës detyrat e punës të cilat përfshijnë ballafaqim me incidente, konstatimi i cenimit të sigurisë së të dhënave personale dhe vlerësim të rrezikut;

- më pas vlerësohet rreziku për personat fizikë i cili është rezultat nga cenimi i sigurisë së të dhënave personale (probabiliteti, përkatësisht nuk ka rrezik, rrezik ose rrezik të lartë) dhe informohen seksione adekuate në kuadër të organizatës;
- parashtrohet njoftim te organi mbikëqyrës dhe, nëse është e nevojshme, informohen personat fizikë të prekur për cenimit të sigurisë së të dhënave personale;
- në të njëjtën kohë kontrolluesi ndërmerr veprim ta ndërpresë dhe ta korrigjojë cenimin e sigurisë së të dhënave personale;
- cenimi i të dhënave personale dokumentohen paralelisht me zhvillimin e ngjarjeve dhe aktiviteteve.

Është e qartë se kontrolluesi ka detyrim të veprojë sipas të gjitha alarmet iniciale dhe të konstatojë nëse me të vërtetë ka ndodhur cenimi i sigurisë së të dhënave personale. Kjo periudhë e shkurtë i lejon të hetojë rastin dhe të mbledhë prova dhe informata tjera relevante për ngjarjen. Megjithatë , pasi që kontrolluesi ka konstatuar, me nivel të arsyeshëm të sigurisë, se ka ndodhur cenimi i sigurisë së të dhënave personale dhe nëse janë plotësuar kushtet nga neni 37 paragrafi (1) nga LMDHP, ai duhet menjëherë dhe më së voni në afat prej 72 orësh e njofton organin mbikëqyrës. Nëse kontrolluesi nuk paraqet njoftim në periudhën e caktuar kohore dhe nëse është evidente se me të vërtetë ka ndodhur cenimi i sigurisë së të dhënave personale, ajo konsiderohet për të pa harmonizuara me dispozitat për paraqitje të njoftimit nga neni 37 nga LMDHP.

Dispozitat nga neni 36 nga LMDHP qartë udhëzon në detyrimin e kontrolluesit dhe përpunuesit të zbatojnë masa adekuate teknike dhe organizative që të sigurojnë nivel të sigurisë së të dhënave personale që përgjigjet në rrezik, respektivisht masa të cilat mundësojnë zbulim në kohë, ballafaqim me dhe paraqitjen e cenimit të sigurisë së të dhënave personale, konsiderohen për elemente esenciale të këtyre masave.

2.1.3. Kontrollues të përbashkët

Neni 30 nga LMDHP ka të bëjë me kontrolluesit e përbashkët dhe përcakton se ato së bashku i përcaktojë përgjegjësitë e tyre për arritjen e harmonizimit me ligjin. Ajo nënkupton edhe shpërndarje të përgjegjësisë për harmonizim me dispozitat nga neni 37 dhe neni 38 nga LMDHP. Rekomandohen marrëveshje që i lidhin kontrolluesit e përbashkët të përmbajnë dispozita të cilat përcaktojnë cili nga kontrolluesit do të jetë përgjegjës për harmonizimin me detyrimet për parashtrim të njoftimit për cenimin e sigurisë së të dhënave personale.

2.1.4. Detyrime të përpunuesit

Kontrolluesi e mban përgjegjësinë gjithëpërfshirëse për mbrojtjen e të dhënave personale, por përpunuesi ka rol të rëndësishëm në mundësimit të kontrolluesit t'i

plotësojë detyrimet e tij që përfshijnë edhe njoftim për cenimin e sigurisë së të dhënave personale. Neni 32 paragrafi (3) nga LMDHP përcakton se përpunimi nga ana e përpunuesit rregullohet me marrëveshje ose me akt tjetër juridik. Më tej, neni 32 paragrafi (3) alineja gj) përcakton se në marrëveshje ose akt tjetër juridik rregullohet se përpunuesi "ndihmon kontrolluesin për të siguruar harmonizimin e detyrimeve në pajtim me nenet nga 36 deri 40 të këtij ligji, duke marrë parasysh natyrën e përpunimit dhe informacioneve që janë të arritshme për përpunuesin". Neni 37 paragrafi (2) nga LMDHP qartë përcakton se pasi që përpunuesi ka kuptuar për cenimin e sigurisë së të dhënave personale, ai duhet "menjëherë" e njofton kontrolluesin për të njëjtën. Duhet të theksohet se përpunuesi nuk duhet së pari ta vlerësojë probabilitetin nëse cenimi do të rezultojë në rrezik para se ta njoftojë kontrolluesin, por kontrolluesi është ai që e bën këtë vlerësim pasi të kuptojë për cenimin e sigurisë së të dhënave personale. Me fjalë tjera, përpunuesi duhet të konstatojë nëse ka ndodhur cenimi i sigurimi i të dhënave personale dhe ta njoftojnë kontrolluesi. Kontrolluesit shfrytëzojnë përpunuesi që t'i arrijnë qëllimet e tyre të përpunimit, prandaj konsiderohet se kontrolluesi " ka kuptuar" për cenimin e sigurisë pasi që ka qenë i njoftuar për të njëjtën nga ana e përpunuesit. Detyrimi i përpunuesit për njoftim i mundëson kontrolluesit të ballafaqohet me cenimi e sigurisë së të dhënave personale dhe të konstatojë nëse ka nevojë për dorëzimin e njoftimit te organi mbikëqyrës, në pajtim me nenin 37 paragrafi (1) dhe te personal fizik të prekur në pajtim me nenin 38 paragrafi (1) nga LMDHP. Kontrolluesi mund ta hetojë cenimin sepse përpunuesi nuk është në pozitë t'i dijë të gjitha faktet relevante për situatën konkrete, për shembull, kur kontrolluesi ka kopje ose rezervë të kopjes nga të dhënat personale të cilat kanë qenë të shkatërruara ose të humbura nga ana e përpunuesit. Ajo mund të ndikojë mbi vendimin e kontrolluesit nëse duhet të parashtrojë njoftim. LMDHP nuk përcakton afat kohor në të cilën përpunuesi duhet ta alarmojë kontrolluesin, përveç atë se kontrolluesi duhet të njoftohet "menjëherë".

Prandaj, rekomandohet përpunuesit menjëherë ta informojnë kontrolluesin dhe gradualisht të sigurojnë informacione plotësuesen për cenimin e sigurisë së të dhënave personale, pasi që informacionet e tilla do të bëhen të qasshme. Kjo është e rëndësishme dhe i ndihmon kontrolluesve ta plotësojnë detyrimin për parashtrim të njoftimit te organi mbikëqyrës në afat prej 72 orëve. Siç ishte theksuar më lartë, marrëveshja mes kontrolluesit dhe përpunuesit duhet ta precizojë mënyrën në të cilën plotësohen kërkesat nga neni 37 paragrafi (2) në mënyrë plotësuese të dispozitave tjera nga LMDHP. Ajo mund të përfshijë kërkesën për njoftim të hershëm nga ana e përpunuesit në përkrahje të obligimit të kontrolluesit për njoftim të organin mbikëqyrës në afat prej 72 orëve. Kur siguron shërbime për më shumë kontrollues të cilët janë prekur nga incidente të njëjtë, përpunuesi duhet t'i informojë të gjithë kontrolluesit në veçanti për detalet e ngjarjes.

Përpunuesi mund ta parashtrojë njoftimin në emër të kontrolluesit kur ajo ka autorizim paraprak dhe kur ajo është pjesë e marrëveshjes mes kontrolluesit dhe përpunuesit. Njoftimi i tillë duhet të dorëzohet në pajtim me nenin 37 dhe nenin 38 nga LMDHP. Megjithatë , duhet të mbahet mend se detyrimi ligjor për njoftimin mbetet tek kontrolluesi.

2.2. Sigurimi i informacioneve të AMDHP

2.2.1. Informacionet që duhet të sigurohen

Pajtim me nenin 37 paragrafi (3) të LMDHP, gjatë paraqitjes së njoftimit te organi mbikëqyrës, kontrolluesi duhet, si minimum, t'i sigurojë informacionet si vijojnë:

> përshkrimin e natyrës së cenimit të sigurisë së të dhënave personale, përfshirë kategoritë dhe numrin e përafërt të subjekteve të të dhënave personale të tanguar, si dhe kategoritë dhe numrin e përafërt të të përmbledhjeve të tanguara të të dhënave personale;
>
> (b) shënimin e emrit/mbiemrit dhe të dhënave kontaktuese të oficerit për mbrojtjen e të dhënave personale ose të personit tjetër për kontakt, nga i cili mund të merren më shumë informata;
>
> (c) përshkrimin e pasojave të mundshme nga cenimi i sigurisë së të dhënave personale;
>
> (ç) përshkrimin e masave të ndërmarra ose të propozuara nga ana e kontrolluesit për ballafaqim me cenimin e sigurisë së të dhënave personale duke përfshirë edhe masa përkatëse për zvogëlimin e efekteve negative të mundshme.

LMDHP nuk i definon kategoritë e subjektit të të dhënave personale ose kategoritë e regjistrimeve të të dhënave personale. Megjithatë , rekomandohet kontrolluesit t'i theksojnë kategoritë e subjektit të të dhënave personale të drejtohen për persona të ndryshëm fizik të dhënat e secilëve janë prekur me cenimin e sigurisë: në varësi nga deskriptorët që shfrytëzohen, mes tjerash, ato mund të përfshijnë fëmijë dhe grupe të ndryshme, persona me pengesa, të punësuar ose klientë. Edhe regjistrimet të të dhënave personale mund të drejtojnë informacione të ndryshme të cilat kontrolluesi i përpunon, siç janë: të dhëna lidhur me shëndetin, regjistrimet arsimore, informacione për mbrojtje sociale, informacione financiare, llogari bankare, numri i pasaportës dhe tjera.

Mungesa e informacioneve precize (p.sh. numri i saktë i subjektet e prekura të të dhënave personale) nuk duhet të jetë pengesë për dorëzim në kohë të njoftimit për cenimin e sigurisë së të dhënave personale. LMDHP lejon dhënien e informacioneve të përafërta në raport të numrit të personave fizikë të prekur dhe numri i regjistrimeve të të dhënave personale. Fokusi duhet të jetë në ballafaqimin me efektet negative nga cenimi në vend të sigurimit të numrit preciz. Nga këtu, kur është e qartë se ka ndodhur cenimi i sigurisë së të dhënave personale, por ende nuk dihet përfshirja e të njëjtës, që ta plotësojë detyrimin për njoftim më të sigurt është kontrolluesi të parashtrojë njoftim në faza (shih më poshtë).

Neni 37 paragrafi (3) nga LMDHP përcakton se njoftimi duhet të sigurojë minimum informacione të përcaktuara me ligj, kurse kontrolluesi mund të vendosë të dorëzojë detale plotësuese, kur ajo është e nevojshme. Llojet e ndryshme të njoftimit për cenimin e sigurisë së të dhënave personale (mundësia , integriteti ose arritshmëria) mund të imponojnë dorëzim të informacioneve plotësuese për sqarim të tërësishëm të rrethanave në çdo rast në veçanti.

E rëndësishme: Si pjesë e njoftimit te AMDHP, kontrolluesi mund të konsiderohet se është e favorshme të theksojë emrin e përpunuesit nëse burimi i cenimit të sigurisë së të dhënave personale është locuar tek përpunuesi, përveç nëse ajo ka sjellë deri në incident të cilin e tangojnë edhe përmbledhjet e të dhënave personale të kontrolluesve tjerë të cilët i shfrytëzojnë shërbimet e përpunuesit.

Në çdo rast, organi mbikëqyrës mund të kërkojë më shumë detale si pjesë e hetimit që e zbaton për cenimin e sigurisë së të dhënave personale.

2.2.2. Njoftimi në faza

Në varësi të natyrë së cenimit të sigurisë së të dhënave personale, kontrolluesi mund të konsiderojë se është e nevojshme të zbatohet hetim i më tejshëm për përcaktimin e të gjitha fakteve relevante të cilat kanë të bëjnë me incidentin. Konkretisht, neni 37 paragrafi (4) nga LMDHP përcakton:

"Kur edhe vetëm kontrolluesi nuk mund në të njëjtën kohë t'i dorëzojë të gjitha informacionet, ato mund të sigurohen gradualisht (në faza) pa prolongim të më tejshëm."

Kjo do të thotë se LMDHP pranon se kontrolluesi nuk do t'i ketë çdo herë të gjitha informacionet e nevojshme për cenimin e sigurisë të të dhënave personale në afat prej 72 orëve pasi ka kuptuar për të njëjtën sepse në periudhën iniciale nuk janë të arritshme tërësisht dhe përfshirë në detale për incidentin, për këto arsye, lejon njoftimi të dorëzohet në faza (gradualisht). Sigurisht se kjo do të jetë rast me cenimit më të komplikuara të sigurisë së të dhënave personale, siç janë llojet e cenimeve kibernetike të cilat imponojnë hetim forenzik që të konstatohet tërësisht natyra e cenimit dhe shkalla e kompromet imit të të dhënave personale. Në vijim, në shumë raste kontrolluesi do të duhet në mënyrë plotësuese ta hetojë cenimin dhe të dorëzojë informacione plotësuese në fazë më të vonshme. Njoftimi i tillë është lejuar, por vetëm nëse kontrolluesi i arsyeton arsyet për vonesën në pajtim me nenin 37 paragrafi (1) nga LMDHP. Prandaj rekomandohet kontrolluesi së pari të dorëzojë njoftim te AMDHP edhe kur ende nuk i ka informacionet e nevojshme dhe të informojë se më shumë detaje do të jenë të dorëzuara më vonë. AMDHP duhet të caktojë si dhe kur duhet të dorëzohen informacione plotësuese. Ajo nuk e pengon kontrolluesin të sigurojë informacione të më tejshme në cilën do fazë tjetër nëse ka kuptuar në mënyrë plotësuese detale të cilat janë relevante për cenimin e sigurisë së të dhënave personale dhe duhet të dorëzohet te AMDHP.

Fokusi i obligimit për njoftimin e cenimit të të dhënave personale është t'i nxitë kontrolluesit shpejtë të veprojnë dhe ta ndërpresin cenimin, t'i kthejnë të dhënat personale kompromet uese kur ajo është e mundshme, dhe të kërkojnë këshillë nga AMDHP. Njoftimi i AMDHP në 72 orët e para i mundëson kontrolluesit të sigurohet se vendimi nëse ka nevojë ta informohen edhe personat fizikë është e drejtë.

Megjithatë , qëllimi i njoftimit të AMDHP nuk është të merren udhëzime për atë nëse duhet të informohen personat fizikë të prekur. Në disa raste, për shkak të natyrës së cenimit dhe seriozitetit të rrezikut të kontrolluesit duhet menjëherë t'i informojë personat fizikë të prekur. Për shembull, nëse ekziston kërcënim i drejtpërdrejtë për vjedhje të identitetit ose nëse kategori të posaçme të të dhënave personale janë zbuluar onlajn, kontrolluesi duhet menjëherë duhet të ndërmarrë veprime që ta ndërpresë cenimin e sigurisë dhe të njoftojë personat fizikë të prekur. Në rrethana të jashtë zakonshme, informimi i personave fizikë mund të ndodhë para njoftimit të organit mbikëqyrës. Në përgjithësi, njoftimi te AMDHP nuk mund të jetë arsyetim për mos informim të subjektit të të dhënave personale për cenimin e sigurisë së të dhënave personale, kur ajo është e nevojshme.

Është e qartë se pas parashtrimit të njoftimit paraprak, kontrolluesi mund të dorëzojë informacione të azhurnuara te AMDHP nëse hetimi vijues që është zbatuar ka zbuluar se incidenti i sigurisë është ndërprerë dhe nuk ka ndodhur cenim i sigurisë së të dhënave personale. Më pas këto informacione mund t'i plotësojnë informacionet që veç më janë dhënë në AMDHP dhe të shënohet se incidenti nuk ka paraqitur cenim të sigurisë së të dhënave personale. LMDHP nuk përcakton sanksion për paraqitjen e incidentit për të cilën në fund është konstatuar se nuk paraqet cenim të sigurisë së të dhënave personale.

Shembull:
Kontrolluesi e njofton organin mbikëqyrës në afat prej 72 orëve pas zbulimit të cenimit të sigurisë së të dhënave personale për shkak të humbjes së USB pajisjes në të cilën ruhen të dhënat personale të një pjese të klientëve. Më vonë zbulohet se USB pajisja është vendosur në vend të gabuar në hapësirat e kontrolluesit. Kontrolluesi e njofton organin mbikëqyrës për të njëjtën dhe kërkon ndryshim të njoftimit paraprak.

2.2.3. Njoftimi i vonuar

Neni 37 paragrafi (1) nga LMDHP qartë cakton se kur te organi mbikëqyrës nuk është dorëzuar njoftim në afat prej 72 orëve, i njëjti duhet të shoqërohet me sqarim për vonesën. Kjo, së bashku me konceptin për njoftim gradual (në faza), e pranon faktin se kontrolluesit nuk do të jenë në mundësi të dorëzojnë njoftim në periudhën e caktuar kohore, dhen prandaj lejohet njoftim i vonuar.

Për shembull, skenari i tillë mund të ndodhë kur, në periudhë të shkurtë kohore, kontrolluesi ballafaqohet me më shumë cenime të ngjashme të besueshmërisë të të dhënave personale të cilat në mënyrë të njëjtë ndikojnë në numër të madh të subjekteve të të dhënave personale. Kontrolluesi mund të kuptojë për ndonjë cenim dhe nëse e fillon hetimin e tij, kurse para se ta parashtrojë njoftimin, konstaton cenimi të ngjashme të njëpasnjëshme nga arsye të ndryshme. Në varësi të rrethanave, kontrolluesit mund t'i duhet kohë e caktuar që ta konstatojë vëllimin e cenimit dhe, në vend të paraqesë njoftim për çdo cenim në veçanti, kontrolluesi organizon njoftim të rëndësishëm i cili përfshin disa cenime shumë të ngjashme, por për arsye të ndryshme. Kjo mund të sjellë

deri në prolongim të njoftimit te organi mbikëqyrës për më shumë se 72 orë pasi që kontrolluesi së pari ka kuptuar për cenimet e tilla të sigurisë së të dhënave personale.

Në përgjithësi, çdo cenim i veçantë i sigurisë së të dhënave personale është incident që duhet të paraqitet veçanërisht. Megjithatë , që të shmanget mbingarkim i madh, kontrolluesit mund të parashtrojnë njoftim "të bashkuar" që i përfshin të gjitha cenimet, me kusht ato të kenë të bëjnë në lloj të njëjtë të cenimit të sigurisë së të dhënave personale në periudhë relativisht të shkurtë kohore. Nëse ka ndodhur seri e cenimeve të cilat kanë të bëjnë në lloje të ndryshme të të dhënave personale, por cenimi ka ndodhur në mënyrë tjetër, atëherë njoftimi duhet të parashtrohet në mënyrë standarde, respektivisht çdo cenim paraqitet veçanërisht në pajtim me nenin 37.

Edhe pse LMDHP lejon prolongim të njoftimit deri në shkallë të caktuar, ajo nuk duhet konsiderohet për diçka që rregullisht ndodh. Duhet të theksohet se grupi i njoftimit mund të bëhet edhe për më shumë cenime të ngjashme të cilat paraqiten në afat prej 72 orëve.

2.3. Kushte kur nuk është i nevojshëm njoftimi për cenimin e sigurisë së të dhënave personale

Neni 37 paragrafi (1) nga LMDHP qartë thekson se kur "nuk ekziston besueshmëri që cenimi i sigurisë së të dhënave personale do të rezultojë në rrezik për të drejtat dhe liritë e individëve", atëherë nuk ka nevojë për dorëzimin e njoftimit te AMDHP. Shembuj për atë mund të jetë situata në të cilën të dhënat personale veç më janë publikisht të arritshme dhe zbulimin e atyre të dhënave nuk nënkupton rrezik për personat fizik.

Cenimi i besueshmërisë të të dhënave personale të cilat kanë qenë të kriptuara me teknologji më bashkëkohore megjithatë paraqet cenim të sigurisë së të dhënave personale dhe për të njëjtën duhet të paraqitet njoftim. Megjithatë , nëse mundësia e çelësit për dekriptim nuk është ndryshuar, respektivisht çelësi nuk është kompromet uar si pjesë nga cenimi i sigurisë dhe ka qenë gjeneruar në mënyrë e cila lejon qasje te të dhënat me mjete teknologjike të arritshme nga ana e personi i cili nuk ka autorizim të tillë, të dhënat në parim janë të palexueshme. Nga këtu, nuk është e besueshme se cenimi i sigurisë së të dhënave personale do të ketë efekt negativ mbi personat fizikë dhe prandaj nuk ka nevojë ato të jenë të informuar. Prandaj, edhe kur të dhënat personale janë të kriptuara, humbja e tyre ose ndryshimi mund të ketë pasoja negative për subjektet e të dhënave personale nëse kontrolluesi nuk ka kopje rezervë adekuate. Në rast të tillë, subjektet e të dhënave personale duhet të jenë të informua, edhe kur janë zbatuar masa adekuate për kriptim të të dhënave.

Kjo do jetë rast edhe kur të dhënat personale, siç janë fjalëkalime, nuk janë përpunuar në mënyrë të sigurt me funksionin për kuptim dhe kriposje (hashing and salting), me ç'rast hesh-vlera është llogaritur me funksionin më të ri kriptografik për çelësa, çelësi që është shfrytëzuar për kuptim nuk ka qenë i kompromet uar me cenimin dhe çelësi që është shfrytëzuar për kuptimin e të dhënave ka qenë i gjeneruar në mënyrë të njëjtë e

cila nuk mund të jetë e deshifruar me mjetet teknologjike të arritshme nga ana e personit i cili nuk ka autorizim të tillë.

Vijimisht, nëse të dhënat personale janë bërë të palexueshme për palët e paautorizuara dhe kur të dhënat janë kopje ose ekziston kopje rezervë nga të njëjtat, për cenimin e sigurisë së të dhënave personale të kriptuara në mënyrë adekuate nuk duhet të parashtrohet njoftim te organi mbikëqyrës. Njoftimi nuk është i nevojshëm sepse nuk ekziston besueshmëri se cenimi paraqet rrezik për të drejtat dhe liritë e të dhënave personale. Gjithsesi, kjo do të thotë se edhe personat fizikë nuk duhet të jenë të informuar sepse nuk ekziston rrezik i lartë. Por, duhet të kihet parasysh se, edhe pse në fillim nuk ka pasur nevojë për njoftim për shkak të mosekzistimit të mundësisë për paraqitjen e rrezikut për të drejtat dhe liritë e personave fizikë, kjo mund të ndërrohet me kalimin e kohës dhe rreziku duhet të vlerësohet nga fillimi. Për shembull, nëse më vonë zbulohet se çelësi ka qenë i kompromet uar ose nëse zbulohet ndjeshmëri e caktuar e softuerit për kriptim, kontrolluesi megjithatë mund të ketë detyrim për njoftim.

Duhet të vërehet se nëse ndodh cenimi i sigurisë së të dhënave personale dhe nuk ekziston kopje rezervë nga të dhënat e kriptuara, atëherë bëhet fjalë për cenim të arritshmërisë së të dhënave personale që mund të shkaktojnë rrezik për personat fizikë dhe është e nevojshme ata të jenë të njoftuar. Ngjashëm, kur cenimi përfshin humbjen e të dhënave personale të kriptuara dhe ekziston kopje rezerve nga të dhënat personale, ajo duhet të nënshtrohet në detyrimin për njoftimin në varësi të kohës e cila është e nevojshme për kthimin e të dhënave personale nga kopja rezervë dhe efektin nga paarritshmëria e të dhënave personale mbi personat fizikë. Sipas nenit 36 paragrafit (1) alinesë v) nga LMDHP, faktor i rëndësishëm i të dhënave personale është " aftësia për vendosje në kohë, të sërishme të arritshmërisë së të dhënave personale dhe qasjes në to në rast të incidentit fizik ose teknik".

Shembull:
Cenimi i sigurisë së të dhënave personale që nuk imponon njoftim te AMDHP mund të jetë humbja e pajisjes mobile të kriptuar të siguruar që e shfrytëzon kontrolluesi dhe personeli i tij. Me kusht që çelësi për dekriptim të ketë mbetur në pronësi të sigurt të kontrolluesit dhe ajo të mos jetë kopja e vetme e të dhënave personale, sulmuesi nuk mund të qaset te ato. Kjo do të thotë se nuk ekziston probabilitet cenimi të rezultojë me rrezik të lartë për të drejtat dhe liritë e subjekteve të prekura të të dhënave personale. Nëse më vonë bëhet evidente se çelësi për dekriptim ka qenë i kompromet uar ose se softueri/algoritmi për kriptim është i cenueshëm, rreziku për të drejtat dhe liritë e personave fizikë do të ndërrohet dhe në situatë të tillë mund të ekzistojë detyrim për njoftim.

Gjithsesi, nëse kontrolluesi nuk e njofton AMDHP në situatë kur të dhënat personale nuk kanë qenë të kriptuara sigurt, atëherë konsiderohet se ai nuk e ka plotësuar detyrimin nga neni 37 nga LMDHP. Nga këto arsye, kur e zgjedhin softuerin për kriptim kontrolluesit duhet ta vlerësojnë me vëmendje kualitetin dhe zbatimin adekuat të kriptimit të ofruar, që ta kuptojnë nivelin e mbrojtjes që e siguron dhe nëse ai nivel

është adekuat për rreziqet të cilat ekzistojnë. Kontrolluesit duhet të jenë të njoftuar edhe me specifikat e prodhimit të tyre për kriptim. Për shembull, një pajisje mund të jetë kriptuar pasi që është shkyçur, por jo derisa është në gjendje kur është në pushim. Disa prodhime për kriptim kanë "çelësa standarde" të cilat duhet të jenë të ndërruar nga klienti që të jenë efektiv. Ekspertët për siguri mund të konsiderojnë se, në momentin e dhënë, kriptimi është adekuat, por e njëjta mund të mbetet e vjetërsuar për disa vite dhe e hap çështjen nëse të dhënat do jenë mjaftueshëm të kriptuara/sigurta me prodhimin e dhënë dhe nëse ai siguron nivel adekuat të mbrojtjes.

3. NENI 38: INFORMIMI I SUBJEKTIT TË TË DHËNAVE PERSONALE

3.1. Informimi i personave fizikë

Në raste të caktuara, përveç njoftimit te organi mbikëqyrës, kontrolluesi duhet t'i informojë edhe personat fizikë të prekur për cenimin e sigurisë së të dhënave personale.

Neni 38 paragrafi (1) nga LMDHP përcakton:
"Në rast të cenimit të sigurisë së të dhënave personale, i cili ekziston mundësi që të shkaktojë rrezik të lartë për të drejtat dhe liritë e personave fizikë, kontrolluesi, menjëherë e njofton subjektin e të dhënave personale për cenimin."

Kontrolluesit duhet të mbajnë mend se njoftimi i AMDHP-së është i detyrueshëm përveç nëse nuk ekziston mundësi se cenimi i sigurisë së të dhënave personale do të rezultojë në rrezik për të drejtat dhe liritë e personave fizikë, dhe ata duhet të jenë të informuar. Përveç kësaj, kur ekziston probabilitet se cenimi i sigurisë së të dhënave personale do të rezultojë me rrezik të lartë për të drejtat dhe liritë e personave fizikë, dhe ata duhet të jenë të informuar. Nga këtu, pragu për informim të personave fizikë është më i lartë nga ai për njoftim të AMDHP-së dhe jo të gjitha cenimet e sigurisë së të dhënave personale e aktivizojnë detyrimin për informim të personave fizikë, me çka kontrolluesit janë të mbrojtur nga ngarkesat e panevojshme.

LMDHP përcakton se personat fizikë duhet të informohen "menjëherë "për cenimin e sigurisë së të dhënave personale, që do të thotë " sa më shpejtë që mundet". Qëllimi kryesor i informimit të personave fizikë është të sigurojnë informacione konkrete për hapat që duhet t'i ndërmarrin që të mbrohen. Siç është theksuar më lartë, në varësi të natyrës së cenimit të sigurisë së të dhënave personale dhe rrezikun e lidhur, informimi në kohë i personave fizikë do t'i ndihmojë të ndërmarrin hapa që të mbrohen nga pasojat negative që mund të dalin nga cenimi.

3.2. Informacionet që duhen të sigurohen

Gjatë informimit të personave fizikë, neni 38 paragrafi (2) nga LMDHP përcakton se:
"Në njoftimin drejtuar subjektit të të dhënave personale nga paragrafi (1) i këtij neni, në gjuhë të qartë dhe të thjeshtë përshkruhet natyra e cenimit të sigurisë së të dhënave personale dhe si minimum theksohen informatat dhe masat e përmendura në nenin 37 paragrafin (3) pikat (b), (c) dhe (ç) të këtij ligji."

Sipas kësaj dispozite, kontrolluesi duhet t'i sigurojë informacionet si vijojnë:

- përshkrimin e natyrës së cenimit të sigurisë së të dhënave personale;
- emrin dhe kontakt të dhënat e oficerit për mbrojtjen e të dhënave personale ose të personit tjetër për kontakt;

- përshkrimin e pasojave të mundshme nga cenimi i sigurisë së të dhënave personale; dhe
- përshkrimin e masave që janë ndërmarrë ose do të ndërmerren nga ana e kontrolluesit për ballafaqim me cenimin, duke përfshirë edhe masat adekuate për uljen efekteve të mundshme negative.

Si shembull për masat që ndërmerren për ballafaqim me cenimin e sigurisë së të dhënave personale dhe për uljen e efekteve të mundshme negative të cilat kontrolluesi i thekson në njoftimin mund të jetë ajo se, pas parashtrimit të njoftimit te AMDHP ai ka marrë këshilla për menaxhim me cenimin dhe uljen e ndikimit të tij. Gjithashtu, kontrolluesi mund të sigurojë këshilla konkrete për personat fizikë, kur ajo është adekuate, që ato të mbrohen nga pasojat e mundshme negative nga cenimi i sigurisë së të dhënave personale, për shembull: ndryshimi i fjalëkalimit në rast kur janë kompromet uar të dhënat e tyre për lajmërim. Duhet të theksohet se kontrolluesi mund të vendosë të sigurojë edhe informacione plotësuese nga ato të përcaktuara me këtë dispozitë.

3.3. Kontaktimi i personave fizikë

Në parim, subjektet e prekura të të dhënave personale duhet të jenë drejtpërdrejtë të informuar për cenimin relevant të sigurisë së të dhënave personale, përveç nëse ajo nuk nënkupton përpjekje në proporcion jo të duhur nga ana e kontrolluesit. Në rast të tillë, kontrolluesi mund të publikojë njoftim publik ose të zbatojë ndonjë masë tjetër me të cilën subjektet e të dhënave personale janë informuar për mënyrë efektive të barabartë (neni 38 paragrafi (3) alineja v) nga LMDHP).

Gjatë informimit të subjektit të të dhënave personale duhet të shfrytëzohen mesazhe dedikuese dhe ato duhet të dërgohen së bashku me informacione tjera, siç janë azhurnimet e rregullta, informatorë ose mesazhe standarde. Në atë mënyrë, informimi për cenimi e sigurisë së të dhënave personale është e qartë dhe transparente.

Shembuj për metodat transparente të informimit përfshijnë mesazhe direkte (p.sh. e-postë SMS etj) afishe të theksuara ose njoftim në ueb faqe, komunikimi përmes postës ose shpalljeve të theksuara në media të shtypura. Njoftimi i cili është pjesë e njoftimit për opinionin ose blog korporativ nuk konsiderohet mjet efektiv për informim të personave fizikë për cenimin e sigurisë së të dhënave personale. Rekomandohet kontrolluesit të zgjedhin mjete të cilët i maksimizojnë shanset për bartje adekuate të informacioneve te të gjithë personat e prekur fizikë. Në varësi të rrethanave, kjo mund të nënkuptojë shfrytëzim të disa metodave të komunikimit, në vend të një kanali për kontakt.

Gjithashtu, kontrolluesit duhet të sigurohen se njoftimi është i qasshëm në format alternativ adekuat dhe në gjuhë relevante që të sigurohet se personat fizikë i kuptojnë informacionet që u jepen. Për shembull, në përgjithësi konsiderohet se gjuha që është shfrytëzuar gjatë kohës së komunikimeve afariste të rregullta paraprake me personat

fizikë nuk është adekuate për informim të personave për cenimin e sigurisë së të dhënave personale. Me rëndësi esenciale këtu është t'i ndihmohet subjektit të të dhënave personale ta kuptojnë natyrën e cenimit dhe hapat që mund të ndërmerren që të mbrohen.

Kontrolluesit janë në pozicion më të mirë që ta përcaktojnë kanalin më adekuat për informim të personave fizikë për cenimin e sigurisë së të dhënave personale, në veçanti nëse ato shpesh herë janë në kontakt me klientët e tyre. Megjithatë , është e qartë se kontrolluesi duhet të ketë kujdes të mos i shfrytëzojë kanalet për komunikim të cilat kanë qenë të kompromet uara me cenimin e sigurisë sepse edhe ato kanale mund të shfrytëzohen nga ana e sulmuesve të cilët paraqiten si kontrollues.

Nga këto arsye, kontrolluesit mund ta kontaktojnë dhe të konsultohen me AMDHP, jo vetëm që të kërkojnë këshillë në lidhje me informimin e subjektit të të dhënave personale për cenimin në pajtim me 38 nga LMDHP, por edhe për mesazhin përkatës që duhet të dërgohet dhe për mënyrën adekuate për kontaktim të personave fizikë.

Çdo herë kur kontrolluesi nuk është në mundësi t'i informojë personat fizikë për cenimin e sigurisë së të dhënave personale sepse nuk ka mjaftueshëm kontakt informacione për ata, ai duhet t'i informojë menjëherë pasi që të krijohen kushte për të njëjtën (p.sh. kur një person fizik e realizon të drejtën e tij/saj për qasje te të dhënat personale dhe me ç'rast kontrolluesit i siguron informacionet plotësuese të nevojshme për kontakt).

Rregullorja për mënyrën e njoftimit për cenimin e sigurisë së të dhënave personale ("Gazeta Zyrtare e Republikës së Maqedonisë së Veriut" numër 122/20) përmban formular për njoftimin e cenimit të sigurisë së të dhënave personale te subjekti i të dhënave personale dhe te Agjencia, kurse i njëjti është i arritshëm në ueb faqen e AMDHP-së: https://www.dzlp.mk/mk/podzakonski_akti.

3.4. Kushtet të cilat nuk imponojnë informim të personave fizikë

Në nenin 38 paragrafin (3) nga LMDHP janë dhënë tre kushte të cilat, nëse nuk janë plotësuar, nuk e aktivizojnë detyrimin për informim të personave fizikë në rast të cenimit të sigurisë së të dhënave personale: respektivisht:

- kur kontrolluesi ka zbatuar masa përkatëse teknike dhe organizative për mbrojtje dhe ato masa janë zbatuar në lidhje me të dhënat personale të prekura nga cenimi i sigurisë së të dhënave personale, veçanërisht masa që i bëjnë të dhënat personale të kuptueshme për çdo person që nuk ka autorizim për qasje në to, siç është kriptimi;
- kur kontrolluesi ka zbatuar masa plotësuese që garantojnë se tashmë nuk ekziston mundësi për paraqitje të rrezikut të lartë për të drejtat dhe liritë e subjekteve të të dhënave personale nga paragrafi (1) i këtij neni;
- nëse njoftimi kërkon përpjekje joproporcionale nga ana e kontrolluesit. Në atë rast, bëhet njoftimi publik ose zbatohet masa tjetër e ngjashme me të cilën subjektet e të dhënave personale do të informohen barazisht në mënyrë efikase.

Në pajtim me parimin për llogaridhënie, kontrolluesi duhet të jetë në mundësi t'i tregojë AMDHP-së se plotësohet një ose më shumë nga këto kushte. Duhet të theksohet se, edhe pse inicialisht ndoshta nuk ka nevojë për njoftim të tillë sepse nuk ekziston rrezik për të drejtat dhe liritë e personave fizikë, situata e tillë mund të ndryshohet me kalimin e kohës dhe prandaj duhet të bëhet rivlerësim i rrezikut.

Nëse kontrolluesi vendos të mos i informojë personat fizikë për cenimin e sigurisë së të dhënave personale, neni 38 paragrafi (4) nga LMDHP përcakton se AMDHP mund të kërkojë të njëjtën kur konsiderohet besueshmëri se ekziston cenimi dhe të rezultojë me rrezik të lartë për subjektet e të dhënave personale. Në mënyrë alternative, AMDHP mund të konstatojë se janë plotësuar kushtet nga neni 38, paragrafi (3) dhe se nuk ka nevojë për njoftim të personave fizikë. Nëse organi mbikëqyrës konstaton se vendimi i kontrolluesit për të mos i informuar subjektet e të dhënave personale është i pabazë, ai mund të mendojë për zbatimin e autorizimeve të tyre dhe për shqiptimin e sanksioneve.

4. VLERËSIMI I RREZIKUT ME RREZIK TË LARTË

4.1. Rreziku si aktivizues i detyrimit për njoftim

Edhe pse AMDHP vendos detyrim për njoftim të cenimit të sigurisë së të dhënave personale, ajo nuk është e detyrueshme në të gjitha rrethanat:

- njoftimi te organi mbikëqyrës duhet të parashtrohet, përveç në rast kur nuk është e besueshme se cenimi do të rezultojë në rrezik për të drejtat dhe liritë e personave fizikë;
- informimi i personave fizikë për cenimin është i nevojshme vetëm kur ekziston besueshmëri se ajo do të rezultojë me rrezik të lartë për të drejtat dhe liritë.

Kjo do të thotë se menjëherë pasi ka kuptuar për cenimin e sigurisë së të dhënave personale, me rëndësi esenciale është kontrolluesi jo vetëm të tentojë ta ndërpresë incidentin, por edhe ta vlerësojë rrezikun që mund të dalë nga incidenti i tillë. Ekzistojnë dy arsye kryesore për atë: e para, njohuritë për probabilitetin dhe seriozitetin potencial të ndikimit mbi personat fizikë mund t'i ndihmojnë kontrolluesit të ndërmarrë hapa efektiv që ta ndërpresë dhe të ballafaqohet me cenimin, dhe e dyta ajo do të ndihmojë të konstatohet nëse duhet të paraqitet njoftim te organi mbikëqyrës dhe, nëse është e nevojshme, te personat fizikë të prekur.

Siç është theksuar paraprakisht, njoftimi për cenimin e sigurisë së të dhënave personale është i nevojshëm përveç nëse nuk është e besueshme ajo të rezultojë në rrezik për të drejtat dhe liritë e personave fizikë, me ç'rast faktor kryesor për informim të subjekteve të të dhënave personale është probabiliteti se cenimi i sigurisë së të dhënave personale do të rezultojë me *rrezik të lartë* për të drejtat dhe liritë e personave fizikë. Rrezik i tillë ekziston kur cenimi mund të sjellë te dëmi fizik, material ose jomaterial për personat fizikë të dhënat personale të të cilit janë prekur me cenimin e sigurisë. Shembuj për dëme të tilla janë diskriminimi, vjedhja e identitetit dhe mashtrim identiteti, humbja financiare ose cenimi i reputacionit. Kur cenimi përfshin të dhëna personale të cilat zbulojnë orgjinë etnike, qëndrime politike, bindje fetare ose religjioze, ose anëtarësim në sindikata, ose kur përfshin të dhëna gjenetike, të dhëna lidhur me shëndetin ose me jetën seksuale, ose vepra penale dhe dënime penale, ose të dhëna lidhur me masat e sigurisë, dëmi i tillë mund të konsiderohet i të mundshëm.

4.2. Faktorët që duhen të merren parasysh gjatë vlerësimit të rrezikut

Duhet të kihet parasysh se vlerësimi i rrezikut për të drejtat dhe liritë e personave fizikë që është rezultat nga cenimi i sigurisë së të dhënave personale kanë fokus të ndryshëm nga rreziku që shqyrtohet si pjesë nga vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale (VNMDHP). Vlerësimi i ndikimit i merr parasysh rreziqet nga përpunimi i planifikuar i të dhënave personale dhe rreziqet të cilat paraqiten në rast të cenimit të sigurisë. Gjatë shqyrtimit të cenimit potencial të sigurisë së të dhënave personale, vlerësimi i ndikimit që i shqyrton rreziqet më gjenerale dhe në lidhje të besueshmërisë,

si dhe në raport të dëmit që mund të ndodhë për subjektet e të dhënave personale. Me fjalë tjera, ky është vlerësim i ngjarjes hipotetike. Kur bëhet fjalë për cenimin real të sigurisë së të dhënave personale, ngjarja tani më ka ndodhur dhe prandaj fokusi është tërësisht i vënë në rrezikun e rezurtual që e prodhon cenimin mbi personat fizikë.

Shembull:
VNMDHP sugjeron se shfrytëzimi i prodhimit softuerik të propozuar i të sigurisë konkret për mbrojtjen e të dhënave personale paraqet masë adekuate e cila siguron nivel të sigurisë që i përgjigjet rrezikut për personat fizikë nga vetë përpunimi. Megjithatë , nëse më vonë zbulohet se cenueshmëria e prodhimit të tillë, kjo e ndryshon përshtatshmërinë e softuerit për kufizimin e rrezikut për të dhënat personale të mbrojtura dhe i njëjti duhet të vlerësohet sërish si pjesë e vlerësimit të (ri) vijues vlerësim i ndikimit mbi mbrojtjen e të dhënave personale. Më vonë, prekshmëria e tillë e prodhimit është shfrytëzuar dhe ndodh cenim i sigurisë së të dhënave personale.

Kontrolluesi duhet t'i vlerësojë rrethanat konkrete për cenimin, të dhënat e prekura, dhe nivelin potencial të ndikimit mbi personat fizikë, si dhe probabilitetin e rrezikut të tillë të materializohet.
Rekomandohet vlerësimi t'i merr parasysh elementet si vijojnë:

- *Lloji i cenimit të sigurisë së të dhënave personale*

Lloji i cenimit të sigurisë së të dhënave personale që ka ndodhur mund të ndikojë mbi nivelin e rrezikut për personat fizikë. Për shembull, cenimi i besueshmërisë me ç'rast informacione mjekësore janë zbuluar në faqe të paautorizuara mund të ketë pasoja të ndryshme për ndonjë person fizik sesa cenimi i sigurisë për shkak të humbjes së arritshmërisë së dosjes mjekësore të personit.

- *Natyra, ndjeshmëria dhe vëllimi i të dhënave personale*

Kuptohet se lloji dhe ndjeshmëria e të dhënave personale të cilat janë kompromet uar me cenimin e sigurisë janë faktor kryesor për vlerësim të rrezikut. Sa më e madhe ndjeshmëria e të dhënave, aq më i lartë është rreziku për shkaktimin e dëmit të personave që janë prekur, por parasysh duhet të merren edhe të dhëna tjera personale të subjektit të cilat janë të arritshme. Për shembull, i vogël është probabiliteti se zbulimi i emrit dhe adresës së ndonjë personi në rrethana normale do të shkaktojë dëm të konsiderueshëm. Megjithatë , nëse emri dhe adresa e prindit-birësues zbulohen nga prindi biologjik, pasojat mund të jenë shumë serioze edhe për birësuesin edhe për fëmijën.

Cenimet të cilat përfshijnë të dhëna për shëndetin, dokumente për identifikim personal, ose të dhëna ndërkombëtare, për shembull numri i kartelës kreditore, vetvetiu mund të shkaktojnë dëm, por kur shfrytëzohen së bashku mund të sjellin edhe te vjedhja e identitetit. Zakonisht, kombinimi i të dhënave personale është më i ndjeshëm nga e dhëna personale individuale.

Në shikim të parë, disa lloje të informatave personale mund të jenë relativisht të sigurta, por gjithsesi me vëmendje duhet të mendohet për atë që të dhënat mund të zbulohen

për personin e prekur. Lista e klientëve të cilët marrin dërgesa të rregullta ndoshta nuk do të konsiderohet për të dhëna veçanërisht të ndjeshme, po të dhënat e njëjta për klientët të cilët kanë kërkuar që dërgesa të jetë e stopuar derisa janë në pushim ndoshta do të jetë informacion i favorshëm për kriminel.

Ngjashëm me këtë, vëllim i vogël i të dhënave personale me ndjeshmëri të lartë mund të ketë ndikim të madh mbi ndonjë person, dhe vëllim i madh i detaleve mund të zbulojnë spektër të gjerë të informacioneve për atë person. Gjithashtu, cenimi i sigurisë i cili ka të bëjë me vëllim të madh të të dhënave personale për numër të madh të subjekteve të të dhënave personale mund të ndikojë mbi numër të madh adekuat të personave fizikë.

- *Identifikim i lehtë i personave fizikë*

Faktor i rëndësishëm që duhet të shqyrtohet është lehtësia me të cilën ana që ka qasje te të dhënat personale të kompromet uara që mund të identifikojnë persona të caktuar ose t'i kombinojnë të dhënat me informacione tjera për identifikimin e ndonjë personi. Në varësi të rrethanave, identifikimi është i mundshëm drejtpërdrejtë nga të dhënat personale siguria e secilit është cenuar pa hulumtimin e veçantë për zbulimin e identitetit të personit, ose mund të jetë jashtëzakonisht e vështirë të dhënat personale të lidhen me personin konkret, por megjithatë është e mundur në kushte të caktuara. Është e mundshme identifikimi direkt ose indirekt nga të dhënat personale siguria e të cilave është cenuar, por ajo mund të varet nga konteksti konkret për cenim dhe arritshmëri publike të detaleve personale të lidhura. Kjo situatë është më relevante në rast të cenimit të besueshmërisë dhe arritshmërisë së të dhënave personale.

Siç ishte theksuar paraprakisht, të dhënat personale të cilat janë mbrojtur me nivel adekuat të kriptimit do të jenë të palexueshme për persona të paautorizuar të cilët nuk kanë çelës për dekriptim. Përveç kësaj, zbatimi adekuat i pseudonimizimit (definuar në nenin 4, pika 5) nga LMDHP si "është përpunim i të dhënave personale në mënyrë që të dhënat personale nuk mund të ndërlidhen me subjekt të caktuar të të dhënave personale pa u shfrytëzuar informata shtesë, me kusht që informatat e tilla shtesë të ruhen veçmas dhe t'u nënshtrohen masave teknike dhe organizative me të cilat do të sigurohet që të dhënat personale nuk ndërlidhen me person fizik të identifikuar ose person fizik i cili mund të identifikohet") mund ta ulë probalitetin për identifikim të personave fizikë në rast të cenimit të sigurisë së të dhënave personale. Gjithsesi, përjashton zbatim të teknikave për pseudonimizim nuk mund të konsiderohet për shndërim të të dhënave personale në informacione të palexueshme.

- *Serioziteti i pasojave për personat fizikë*

Në varësi të natyrës të të dhënave personale të cilat janë të prekura me cenimin e sigurisë, dëmi potencial për personat fizikë që është rezultat i cenimit të tillë mund të jetë mjaft serioz, veçanërisht në rast kur cenimi mund të rezultojë me vjedhje të identitetit ose mashtrim identitar, dëmtim fizik, stres psikologjik, nënçmim ose reputacion të prishur. Nëse cenimi ka të bëjë me të dhënat personale për personat e prekur, ato do ishin vënë në rrezik më të madh nga dëmi.

Vetëdija e kontrolluesit për atë nëse të dhënat personale janë në duar të personave qëllimet e të cilëve janë të panjohura ose ndoshta malicioze mund të ndikojnë në nivel të rrezikut potencial. Mund të bëhet fjalë për cenim të besueshmërisë së të dhënave personale, me ç'rast me gabim janë zbuluar nga pala e tretë, ashtu siç është definuar në nenin 4 pikën 10) nga LMDHP, ose të shfrytëzuesi tjetër. Kjo mund të ndodhë, për shembull, kur të dhënat personale rastësisht dërgohen te seksion i gabuar në kuadër të një organizate, ose te furnizuesit i cili zakonisht shfrytëzohet. Kontrolluesi mund të kërkojë nga shfrytëzuesi t'i kthejë ose në mënyrë të sigurt t'i asgjësojë të dhënat që i janë zbuluar. Në të dy rastet, shfrytëzuesi mund të konsiderohet si entitet "nga besimi" duke pasur parasysh atë se kontrolluesi ka raport vijues me atë organizatë ose mund të jetë i njohur me procedurat, historiatin dhe detaje tjera relevante për shfrytëzuesin.

Me fjalë tjera, kontrolluesi mund të konsiderohet në nivel të caktuar të sigurisë se shfrytëzuesi nuk do t'i lexojë ose nuk do të qaset te të dhënat të cilat janë dërguar me gabim dhe se do t'i respektojë instruksionet e dhëna nga kontrolluesi për kthim të të dhënave. Edhe kur shfrytëzuesi është qasur te të dhënat personale, kontrolluesi mund të besojë se nuk do të ndërmarrë veprim tjetër, menjëherë do t'i kthejë kontrolluesit dhe do të bashkëpunojë në drejtim të kthimit të të dhënave. Në rast të tillë, fakti se shfrytëzuesi është entitet i besueshëm mund të merret parasysh në vlerësimin e rrezikut që e zbaton kontrolluesi pas ndodhjes së cenimit, që e ul seriozitetin e pasojave nga cenimi, por nuk do të thotë se nuk ka ndodhur cenimi i sigurisë së të dhënave personale. Për kthim, ajo mund ta largojë besueshmërinë për rrezik të personave fizikë, me çka nuk ka më nevojë për paraqitje të njoftimit te organi mbikëqyrës ose nga personat fizikë të prekur. Duhet të theksohet, nëse ajo do të varet nga rrethanat në rastin konkret. Edhe krahas kësaj, kontrolluesi duhet t'i ruajë informacionet për cenim si pjesë nga detyrimi i përgjithshëm për mbajtjen e evidencës për cenimin e sigurisë së të dhënave personale.

Duhet të kihet parasysh edhe kohëzgjatja e pasojave për personat fizikë, sepse ndikimi mund të konsiderohet më i madh nëse efektet nga cenimi janë afatgjata.

- *Karakteristikat e veçanta të personave fizikë*

Një cenim i sigurisë mund të ndikojë në të dhënat personale të fëmijëve ose grupeve tjera të prekura të cilat mund të jenë të ekspozuara në rrezik më të madh nga cenimi si rezultat i të njëjtës. Ekzistojnë edhe faktorë tjerë të personave fizikë të cilët mund të ndikojnë në nivelin e rrezikut në të cilin janë ekspozuar për shkak të cenimit të sigurisë së të dhënave personale.

- *Karakteristika të posaçme të kontrolluesit*

Natyra dhe roli i kontrolluesit dhe aktivitetet e tij mund të ndikojnë mbi nivelin e rrezikut të personave fizikë i cili është rezultat i cenimit të sigurisë së të dhënave personale. Për shembull, institucionet mjekësore përpunojnë kategori të posaçme të të dhënave personale, që do të thotë ekziston kërcënim më i madh për personat fizikë nëse është cenuar siguria e të dhënave të tyre personale, për dallim nga situata në të cilën përfshin mejling lista e ndonjë organizate gazetareske.

- *Numri i personave fizikë të prekur*

Cenimi i sigurisë së të dhënave personale mund të ndikojnë mbi një, disa ose disa mijëra persona fizikë, ndoshta edhe më shumë. Në përgjithësi, sa më i lartë është numri i personave fizikë të prekur aq më i madh është ndikimi që mund të shkaktojë cenim. Gjithsesi, një cenim mund të ketë ndikim serioz edhe kur vetëm një person fizik në varësi të natyrës së të dhënave personale dhe në kontekst në të cilin janë kompromet uar. Duhet të theksohet se me rëndësi esenciale në këto raste është të konstatohet mundësia dhe serioziteti i ndikimit mbi personat që janë prekur.

- *Qëllimet e përgjithshme*

Një nga këto arsye, gjatë vlerësimit të rrezikut i cili sigurisht do të dalë nga cenimi i sigurisë së të dhënave personale kontrolluesi duhet ta marrë parasysh kombinimin nga serioziteti i ndikimit potencial për të drejtat dhe liritë e personave fizikë dhe mundësia që ajo të realizohet. Qartë është se kur pasojat nga cenimi janë më serioze, rreziku është më i madh. Ngjashëm, kur mundësia për realizimin e ndikimit është më e madhe, ekziston rrezik më i madh. Kur nuk janë të sigurt, kontrolluesit çdo herë duhet të veprojnë nga ana e vëmendjes dhe të paraqesin raport për cenimin e sigurisë së të dhënave personale.

5. LLOGARIDHËNIA DHE MBAJTJA E EVIDENCËS

5.1. Dokumentimi i cenimeve të sigurisë së të dhënave personale

Duke pasur parasysh atë nëse cenimi i sigurisë së të dhënave personale duhet të paraqitet te organi mbikëqyrës, kontrolluesi duhet të mbajë evidencë për të gjitha cenimet e sigurisë së të dhënave personale, që është përcaktuar në nenin 37 paragrafin (5) nga LMDHP:

" Kontrolluesi i dokumenton të gjitha cenimet e sigurisë së të dhënave personale, përfshirë faktet që lidhen me cenimin e sigurisë së të dhënave personale, pasojat e tyre dhe aktivitetet e ndërmarra për ballafaqim me cenimin, në mënyrë që t'i mundësojë Agjencisë ta kontrollojë harmonizimin me këtë nen.
"

Kjo është lidhur me parimin për llogaridhënie nga ligji, i cili është dhënë në nenin 9 paragrafin (2). Qëllimi i mbajtjes së evidencës për cenimet të cilat nuk paraqiten, si dhe për cenimet të cilat duhet të paraqiten, është i lidhur me detyrimin e kontrolluesit të dhënë në nenin 28 nga LMDHP, me ç'rast organi mbikëqyrës mund të kërkojë kontroll në evidencën e tillë.
Nga kjo arsye, këshillohet kontrolluesi të vendosë regjistër intern të cenimeve të sigurisë së të dhënave personale pa marrë parasysh nëse kjo e aktivizon detyrimin për njoftim ose jo.

Edhe pse kontrolluesi vetë vendos për metodën dhe strukturën e evidencës për dokumentim të cenimit të sigurisë së të dhënave personale, kur bëhet fjalë për informacione të cilat duhet të shënohen ekzistojnë disa elemente kryesore që duhet të jenë të përfshira në të gjitha regjistrimet. Në pajtim me nenin 37 paragrafin (5) nga LMDHP, kontrolluesi duhet t'i dokumentojë detajet lidhur me cenimin e sigurisë së të dhënave personale, që përfshin arsyen, kohën kur ka ndodhur cenimi dhe cilat janë të dhënat personale të prekura. Gjithashtu, evidenca duhet të përfshijë edhe efektet dhe pasojat nga cenimit, së bashku me masat kolektive që i ka marrë kontrolluesi.

LMDHP nuk e precizon afatin për ruajtjen e këtij dokumentacioni. Kur regjistrimet e tilla përmbajnë të dhëna personale, nga kontrolluesi pritet të konstatojë afat adekuat për ruajtje në pajtim me parimin i cili ka të bëjë me përpunimin e të dhënave personale dhe duhet të ekzistojë bazë juridike për përpunim. Dokumentacioni nga neni 37 paragrafi (5) nga LMDHP duhet të ruhet sepse AMDHP mund të kërkojë nga kontrolluesi të dorëzojë provë për harmonizim me dispozitat nga ai nen ose në përgjithësi për harmonizim me parimin për llogaridhënie. Nënkuptohet se parimi për kufizim të afatit për ruajtje nuk zbatohet nëse shkresat nuk përmbajnë të dhëna personale.

Në mënyrë plotësuese në këto detaje, rekomandohet kontrolluesit ta dokumentojnë edhe rezonimin e tyre për vendimet që i kanë sjellë si përgjigje për cenimin e sigurisë të sigurisë së të dhënave personale. Konkretisht, nëse nuk parashtrohet njoftim për cenim, duhet të dokumentohet dhe arsyetimi për vendimin tillë. Ajo duhet t'i përfshijë arsyet pse kontrolluesi konsideron se nuk ekziston besueshmëri cenimi të rezultojë në

rrezik të lartë për të drejtat dhe liritë të personave. Në mënyrë alternative, nëse kontrolluesi konsideron se janë plotësuar disa nga kushtet të dhëna në nenin 38 paragrafin (3) nga LMDHP, ai duhet të jenë në mundësi të sigurojë prova adekuate për vendimin e tillë.

Kur kontrolluesi paraqet njoftim për cenim e sigurisë së të dhënave te AMDHP, por gjithashtu është e vonuar, ai duhet të jetë në mundësi t'i theksojë arsyet për vonesë, respektivisht duhet të sigurojë dokumente të cilat tregojnë se vonesa e njoftimit është e arsyeshme dhe nuk është tej mase.

Kur kontrolluesi i informon personat fizikë të prekur për cenimin e sigurisë së të dhënave personale, ai duhet të jetë transparent për cenimin, me ç'rast komunikimi i tillë duhet të jetë efektiv dhe në kohë. Gjithashtu, ruajtja e provave nga komunikimi i tillë i ndihmon kontrolluesit në shfaqje të llogaridhënies dhe harmonizimit.

Për qëllimet e harmonizimit me nenin 37 dhe nenin 38, është e favorshme kontrolluesi dhe përpunuesi të kenë të vendosur procedurë të dokumentuar për njoftim, respektivisht kanë përcaktuar proces të cilin e ndjekin pas zbulimit të cenimit të sigurisë së të dhënave personale, që përfshin edhe procedura për izolim, menaxhim dhe zgjidhjen e incidentit, si dhe për vlerësim të rrezikut, dhe paraqitje të njoftimit. Në këtë kuptim, që të tregohet harmonizimi me ligjin, është e favorshme që kontrolluesit të jenë në mundësi të demonstrojnë se të punësuarit janë njohur me procedurat e tilla dhe mekanizma dhe e dinë si të reagojnë gjatë cenimit të sigurisë së të dhënave personale.

Duhet të theksohet se mos parashtrimi i dokumenteve adekuate për cenim të sigurisë së të dhënave personale mund të sjellë deri në aktivizim të autorizimit të AMDHP në pajtim me nenin 66 nga LMDHP dhe shqiptim të gjobës kundërvajtëse në pajtim me nenin 110.

5.2. Roli i oficerit për mbrojtjen e të dhënave personale

Kontrolluesit dhe përpunuesit mund të kenë caktuar oficer për mbrojtjen e të dhënave personale në pajtim me kërkesat nga neni 41 nga LMDHP ose në bazë vullnetare, respektivisht si praktikë e mirë. Neni 43 nga LMDHP përcakton varg detyrash të detyrueshme për oficerët për mbrojtjen e të dhënave personale, por nuk i kufizon kontrolluesit t'u ndajë detyra tjera të punës, nëse ajo është përkatëse.

Në raport të njoftimit për cenim të sigurisë së të dhënave personale, detyrat e detyrueshme të oficerëve, mes tjerash, përfshijnë dhënien e këshillave dhe informatave të kontrolluesit ose përpunuesit, ndjekjen e harmonizimit me LMDHP, dhe dhënien e këshillave në lidhje me vlerësimin e ndikimit mbi mbrojtjen e të dhënave personale. Oficeri për mbrojtjen e të dhënave personale duhet të bashkëpunojnë me AMDHP dhe të veprojë si pikë kontakti për Agjencinë dhe për subjektet e të dhënave personale. Duhet të shënohet se, gjatë parashtrimit të njoftimit për cenimin e sigurisë së të dhënave personale te organi mbikëqyrës (AMDHP), neni 37 paragrafi (3) pika b) nga LMDHP imponon kontrolluesit ta theksojnë emrin dhe detajet e kontaktit të oficerit të tyre për

mbrojtjen e të dhënave personale ose të personit tjetër i cili është përcaktuar si pikë kontakti.

Nga aspekti i dokumentimit të cenimit të sigurisë së të dhënave personale, kontrolluesit ose përpunuesit mund të kërkojnë mendim nga oficeri i tyre në lidhje me strukturën, organizatën dhe administrimin e këtij dokumentacioni. Oficeri për mbrojtjen e të dhënave personale mund të ketë detyra plotësuese lidhur me ruajtjen e evidencës së tillë.

Këto faktorë udhëzojnë në atë se oficeri për mbrojtjen e të dhënave personale duhet të ketë rol kryesor në dhënien e ndihmës për parandalim ose përgatitje për ballafaqim me cenimin e sigurisë së të dhënave personale përmes këshillave ose ndjekjes së harmonizimit, si dhe për kohën e cenimit (kur njoftohet AMDHP) dhe për kohën e hetimit të njëpasnjëshëm nga ana e AMDHP-së. Në këtë drejtim, rekomandohet oficeri për mbrojtjen e të dhënave personale menjëherë të informohet për ekzistimin e cenimit të sigurisë së të dhënave personale dhe të përfshihet në tërë procedurën për menaxhim me cenimin dhe parashtrimin e njoftimit për cenimin e sigurisë së të dhënave personale.

6. SHEMBUJ PËR CENIM TË SIGURISË SË TË DHËNAVE PERSONALE DHE KUSH DUHET TË NJOFTOHET

Më poshtë është dhënë listë joshteruese me shembuj e cila do t'i ndihmojë kontrolluesve të konstatojnë nëse duhet të parashtrojnë njoftim në skenarë të ndryshëm me cenimin e sigurisë së të dhënave personale. Këta shembuj mund të ndihmojnë në përkufizimin e asaj çka është rrezik, kurse çka është rrezik për të drejtat dhe liritë e personave fizikë.

Shembull	**Njoftim i AMDHP-së?**	**Njoftim i subjektit të të dhënave personale?**	**Shënime/rekomandime**
1. Kontrolluesi shfrytëzon pajisje USB për ruajtjen e kopjes së sigurisë nga arkivi i të dhënave personale të cilat janë kriptuar. Pajisja USB është vjedhur gjatë vjedhjes në hapësirat e kontrolluesit.	Jo.	Jo.	Nëse të dhënat personale janë kriptuar me algoritëm sipas teknologjisë më të re, ekziston kopje rezerve nga të dhënat personale dhe çelësi i vetëm për dekriptim nuk është kompromet uar, të dhënat mund të kthehen për periudhë të shkurtë kohore dhe kjo situatë nuk duhet të paraqitet si cenim i sigurisë së të dhënave personale. Megjithatë , nëse më vonë ato bëhen të kompromet uara atëherë kontrolluesi duhet të paraqesë njoftim
2. Kontrolluesi ofron shërbime onlajn, me ç'rasttë dhënat personale të personave fizikë (klientë) janë nxjerrë si rezultat nga sulmet kibernetike nga shërbime onlajn.	Po, parashtrohet njoftim te AMDHP kur është e besueshme se do të ketë pasoja për personat fizikë.	Po, parashtrohet njoftim te personat fizikë në varësi nga të dhënat personale të cilat janë prekur me këtë sulm dhe nga shkalla e mundësisë për seriozitetin e pasojave për personat fizikë.	
3. Ndërprerje e shkurtë e energjisë elektrike në kohëzgjatje prej disa minutave në qendrën për kujdes të shfrytëzuesit nënkupton se klientët nuk janë në mundësi	Jo.	Jo.	Kjo nuk paraqet cenim të sigurisë që duhet të paraqitet, por duhet të dokumentohet si incident në pajtim me nenin 37 paragrafin (5) nga LMDHP. Kontrolluesi duhet të mbajë evidencë adekuate për këtë.

të paraqiten në shërbimet dhe të marrin qasje te regjistrimet e tyre.			
4. Kontrolluesi është sulmuar me ransomver që rezulton në kriptim të të gjitha të dhënave. Nuk ekziston kopje rezervë dhe të dhënat nuk mund të kthehen. Gjatë hetimit të ngjarjes bëhet e qartë se funksioni i vetëm i sulmit ka qenë kriptimi i të dhënave, por në sistem nuk ekziston softuer tjetër malicioz.	Po, duhet të parashtrohet njoftimi te AMDHP nëse ekziston mundësi për pasojat për personat fizikë sepse bëhet fjalë për humbje të arritshmërisë të të dhënave personale.	Po, duhet të parashtrohet njoftim te personat fizikë në varësi nga natyra e të dhënave personale të prekura dhe efekti i mundshëm nga arritshmëria e të dhënave personale, si dhe mundësia për paraqitje të pasojave tjera.	Nëse ekziston kopje rezervë nga të dhënat personale dhe ato mund të kthehen në një kohë të ardhshme, atëherë nuk ka nevojë për njoftim të AMDHP-së dhe personave fizikë sepse nuk ka humbje të vazhdueshme të arritshmërisë ose besueshmërisë të të dhënave personale. Megjithatë , nëse AMDHP është informuar për këtë incident, ajo mund të mendojë për hetimin e rastit dhe të vlerësohet harmonizimi me masat për siguri të të dhënave personale në pajtim me nenin 36 nga LMDHP.
5. Një person paraqitet në qendrën për informim të bankës që të paraqitet cenimi i sigurisë së të dhënave personale. Personi ka marrë raport mujor nga llogaria bankare e dikujt tjetër. Kontrolluesi zbaton hetim të shkurtë (i cili ka mbaruar në periudhë prej 24 orëve) dhe përcakton me siguri të arsyeshme se ka ndodhur cenimi i sigurisë së të dhënave personale dhe se bëhet fjalë për mungesë sistematike e cila mund të thotë se persona tjerë janë ose mund të jenë prekur me të njëjtën.	Po.	Njoftohen vetëm personat fizikë të prekur nëse ekziston rrezik i lartë dhe qartë është përcaktuar se të tjerët nuk janë prekur.	Nëse pas hetimit përcaktohet se janë prekur më shumë persona, te AMDHP duhet të dërgojë njoftim të azhurnuar dhe kontrolluesi duhet të ndërmarrë hapa plotësues për njoftim të personave tjerë fizikë kur ekziston rrezik i lartë për ata.
6. Kontrolluesi ka shitore onlajn dhe ka numër të madh të klientëve. Shitorja onlajn është cak i	Po, paraqitet njoftim te AMDHP	Po, paraqitet njoftim te subjekti i të dhënave personale sepse ajo mund të sjellë te rreziku i lartë	Kontrolluesi duhet të ndërmarrë veprime për uljen e rrezikut, për shembull, përmes ndryshimit të detyrueshëm të fjalëkalimit të

sulmit kibernetik me ç'rast sulmuesi në internet i publikon emrat e shfrytëzuesve, fjalëkalimet dhe historiatin e prodhimeve të blera të klientit të kontrolluesit.		për ata.	llogarive shfrytëzuese të prekura, dhe hapa tjerë. Kontrolluesi duhet të marrë parasysh edhe detyrimet tjera për njoftim.
7. Kompania e cila siguron hostim të ueb faqeve dhe vepron si përpunues ka identifikuar gabime në kodin për kontrolle të autorizimeve të shfrytëzuesve. Efekti nga gabimi i tillë do të thotë se çdo shfrytëzues mund të qaset te detajet për llogaritë e shfrytëzuesve.	Si përpunues, kompania për hostim të ueb faqes duhet menjëherë dhe pa prolongim t'i njoftojë klientët e prekur (kontrolluesit). Nën supozim se kompania ka zbatuar hetim vetanak, kontrolluesit e prekur duhet të jenë të sigurt në mënyrë të arsyeshme nëse secili nga ata ka pësuar cenim të sigurisë së të dhënave personale dhe sigurisht është se çdo kush nga ata "ka kuptuar" për të njëjtën pasi është informuar nga kompania për hostim të ueb faqes (përpunuesi). Më pas, kontrolluesi duhet të dorëzojë njoftim te AMDHP.	Nëse nuk ekziston besueshmëri për rrezik të lartë të personave fizikë, ata nuk duhet të jenë të njoftuar.	Kompania për hostim në ueb faqen (përpunuesi) duhet të merren parasysh dhe obligimet tjera për njoftim. Nëse nuk ka prova se prekshmëria është shfrytëzuar në raport të ndonjë kontrolluesi që i shërben kompanitë, mund të konsiderohet se nuk ka ndodhur cenim i sigurisë së të dhënave personale e cila imponon njoftim, por sigurisht duhet të dokumentohet ose nënkupton mosharmonizim me nenin 36 nga LMDHP.
8. Për shkak të sulmit kibernetik, dosjet mjekësore të një spitali janë të paarritshme në periudhë prej 30 orëve.	Po, spitali është obliguar të paraqesë njoftim sepse mund të paraqitet rrezik i lartë për mirëqenien dhe privatësinë e pacientëve	Po, njoftohen personat fizikë të prekur.	
9. Me gabim, të dhënat personale të numri të madh të studentëve janë dërguar në mejling listë të gabuar me më shumë se 1000 pranues	Po, parashtrohet njoftim te organi mbikëqyrës.	Po, parashtrohet njoftim te personat fizikë në varësi të vëllimit dhe llojit të të dhënave personale të cilët janë të prekur dhe seriozitetin e pasojave të mundshme.	

10. Imejl marketingu i drejtpërdrejtë është dërguar te pranuesit në fushën për adresa të fshehura, me çka të gjithë mund të shohin adresa elektronike të pranuesve tjerë.	Po, njoftimi i organit mbikëqyrës mund të jetë i detyrueshëm nëse janë prekur numër i madh i personave fizikë, nëse zbulojnë të dhëna të ndjeshme (p.sh. mejling lista e psiko terapeutik) ose nëse faktorë tjerë paraqesin rrezik të lartë (p.sh., e- mejli e përmban fjalëkalimin inicial).	Po, personat fizikë njoftohen në varësi të vëllimit dhe llojit të të dhënave personale të prekura dhe seriozitetin e pasojave të mundshme.	Njoftimi ndoshta nuk do të jetë i nevojshëm nëse janë zbuluar të dhëna të ndjeshme ose nëse janë zbuluar të dhëna të ndjeshme ose nëse janë zbuluar vetëm numër i vogël i adresave elektronike.

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.

SCAN ME

+389 2 3230 635

info@privacy.mk

bul “Goce Dellçev” nr. 18
Shkupi

www.azlp.mk