



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

# UDHËRRËFYES PËR MASAT TEKNIKE DHE ORGANIZATIVE



Ky projekt financohet nga Bashkimi Evropian





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.



Ky projekt financohet nga Bashkimi Evropian



# UDHËRRËFYES

## PËR MASAT TEKNIKE DHE ORGANIZATIVE



## PËRMBAJTJA

<b>1</b>	<b>Çfarë janë të dhënat personale dhe cilat janë bazat juridike për mbrojtjen e të dhënave personale....</b>	<b>3</b>
<b>2</b>	<b>Çfarë janë masat teknike dhe organizative? .....</b>	<b>3</b>
<b>3</b>	<b>Menaxhimi i rrezeve .....</b>	<b>4</b>
<b>4</b>	<b>Dokumentacioni për masat teknike dhe organizative .....</b>	<b>6</b>
<b>5</b>	<b>Masat organizative .....</b>	<b>7</b>
<b>5.1</b>	<b>Niveli standard i masave organizative .....</b>	<b>7</b>
5.1.1	Masat organizative për mbrojtjen e të dhënave personale (standardi minimal).....	7
5.1.1.1	Përcaktimi i personave të autorizuar që kanë qasje në të dhënat personale .....	7
5.1.1.2	Rregullat organizative për qasjen në internet nga personat e autorizuar lidhur me shkarkimin dhe regjistrimin e dokumenteve që shkarkohen nga e-posta ose nga burimet e tjera .....	9
5.1.1.3	Shkatërrimi i dokumenteve pas skadimit të afatit të tyre të ruajtjes .....	10
5.1.1.4	Masat për sigurinë fizike të hapësirave dhe pajisjes informatike dhe të komunikimit në të cilën mblidhen, përpunohen dhe ruhen të dhënat personale .....	11
5.1.1.5	Harmonizimi me udhëzimet teknike për instalimin dhe funksionimin e pajisjes informatike dhe të komunikimit që përdoret për përpunimin e të dhënave personale .....	12
5.1.2	Informimi dhe edukimi për mbrojtjen e të dhënave personale .....	12
5.1.3	Detyrimet dhe përgjegjësitë e administratorit të sistemit informatikë dhe të personave të autorizuar .....	13
5.1.4	Mbrojtja e të dhënave që ruhen në formë letre .....	14
<b>5.2</b>	<b>Niveli i lartë i masave organizative .....</b>	<b>15</b>
<b>6</b>	<b>Masat teknike .....</b>	<b>15</b>
<b>6.1</b>	<b>Niveli standard i masave teknike.....</b>	<b>15</b>
6.1.1	Zbatimi i masave teknike përkatëse për përbushjen e dispozitave për autorizimet për qasje në të dhënat personale .....	15
6.1.2	Sigurimi i pajisjes që përdoret për përpunimin e të dhënave personale .....	18
6.1.3	Mbajtja e evidencës për hyrjet në sistemin informatikë.....	19
6.1.4	Sigurimi i pajisjes së lëvizshme dhe mediumeve të transmetimit.....	21
6.1.5	Sigurimi i rrjetit intern (intranet).....	22
6.1.6	Sigurimi i serverëve .....	25
6.1.7	Sigurimi i ueb-faqeve .....	26
6.1.8	Parandalimi, reagimi dhe kthimi i sistemit pas incidenteve (sigurimi i vazhdimësisë).....	29
6.1.9	Kopjet rezervë dhe kthimi i të dhënave personale (sigurimi i vazhdimësisë) .....	29
6.1.10	Mënyra e arkivimit dhe ruajtjes së të dhënave.....	31
6.1.11	Kriptimi i të dhënave personale .....	32
6.1.12	Shkëmbimi i të dhënave përmes postës elektronike .....	33
6.1.13	Siguria fizike .....	34
6.1.14	Kontrollimi i sistemit informatikë dhe infrastrukturës.....	36
6.1.15	Menaxhimi i përpunuesve dhe angazhimi i përpunuesve.....	36
<b>6.2</b>	<b>Niveli i lartë i masave teknike .....</b>	<b>37</b>





## 1 Çfarë janë të dhënat personale dhe cilat janë bazat juridike për mbrojtjen e të dhënave personale

Ligji për mbrojtjen e të dhënave personale (në tekstin e mëtejshëm: LMDHP) (“Gazeta Zyrtare e Republikës së Maqedonisë së Veriut” nr.42/20) definojnë se të dhëna personale janë çdo informacion që ka të bëjë me personin e identifikuar ose personin fizik që mund të identifikohet (subjekti i të dhënave personale), ndërsa personi fizik që mund të identifikohet është personi, identiteti i të cilit mund të përcaktohet drejtpërdrejt ose indirekt, veçanërisht në bazë të identifikuesve, siç janë emri dhe mbiemri, numri i amzës i qytetarit, të dhënat për lokacionin, identifikuesit përmes internetit, ose në bazë të një ose më shumë shenjave konkrete për identitetin e tij fizik, fiziologjik, gjenetik, mental, ekonomik, kulturor ose social.

Përveç kësaj, LMDHP-ja definojnë edhe disa kategori të veçanta të të dhënave personale, respektivisht të dhëna që zbulojnë përkatësinë racore ose etnike, qëndrimet politike, fetare ose bindjet filozofike dhe anëtarësinë në sindikata, si dhe të dhëna gjenetike, të dhëna biometrike, të dhëna për shëndetin ose të dhëna për jetën seksuale ose orientimin seksual. Këto të dhëna nuk guxojnë të përpunohen, përveç kur përmbushen kushtet e dhëna në përputhje me nenin 13, paragrafi (2) të LMDHP-së.

Më tutje, LMDHP-ja përcakton se të gjitha organizatat janë të detyruara që të zbatojnë masa teknike dhe organizative përkatëse për mbrojtjen e të dhënave personale, varësisht nga kategoria e të dhënave personale, konteksti, qëllimi për të cilin mbledhen dhe përpunohen të dhënat, si dhe rreziqet e mundshme nga humbja ose keqpërdorimi i të dhënave.

Në përputhje me nenin 66, paragrafi (6) të LMDHP-së, drejtori i Agjencisë për Mbrojtjen e të Dhënave Personale (në tekstin e mëtejshëm: AMDHP) miraton **Rregullore për sigurinë e përpunimit të të dhënave personale** (në tekstin e mëtejshëm: Rregullore), e cila përcakton udhëzimet për aktivitetet që duhet t’i ndërmarrin kontrollorët dhe përpunuesit për zbatimin e masave teknike dhe organizative për mbrojtjen e përpunimit të të dhënave personale.

## 2 Çfarë janë masat teknike dhe organizative?

Siç u theksua më lartë, LMDHP-ja përcakton se të gjitha organizatat janë të detyruara që të zbatojnë masa teknike dhe organizative përkatëse për mbrojtjen e të dhënave personale, varësisht nga vëllimi dhe kategoria e të dhënave personale, konteksti, qëllimi për të cilin mbledhen dhe përpunohen të dhënat dhe rreziqet e mundshme nga humbja ose keqpërdorimi i të dhënave.

Masat teknike mund të definojnë si masa që kontrollorët dhe përpunuesit i zbatojnë në sistemet e tyre dhe në të gjitha mjetet teknologjike të organizatës, siç janë: objektet / ndërtesat, pajisjet, rrjetet, harduerët dhe të dhënat në letër që ata i përdorin si masa për mbrojtje nga qasja e paautorizuar në të dhënat personale dhe mbrojtja më e mirë e mundshme nga cenimi i sigurisë së të dhënave personale. Shembuj për masat teknike janë siguria-kibernetike, kriptimi dhe pseudonimizimi, siguria fizike, menaxhimi përkatës me të dhënat, fjalëkalimet, autorizimet për qasje në të dhënat, etj., ku ato janë përcaktuar edhe me Rregullore.





Masat organizative mund të definojnë si masa që i përbëjnë politikat interne, metodat ose standardet organizative, si dhe kontrollimet dhe hetimet që kontrollorët dhe përpunuesit i përcaktojnë për zbatim, me qëllim që të garantohet siguria e të dhënave personale. Shembuj për masat organizative janë politikat për sigurinë informatike, planin për vazhdimësinë e aktivitetit zyrtar, politikat dhe procedurat për të gjitha llojet e përpunimit të të dhënave personale në kuadër të organizatës, krijimi i vetëdijes dhe trajnimit për punonjësit, kontrollimet dhe revizionet e masave të përcaktuara dhe të zbatuara, etj... Edhe këto masa janë të përcaktuara me Rregullore.

Arsyeja pse kontrollorët dhe përpunuesit duhet t'i zbatojnë masat teknike dhe organizative përkatëse qëndron në nevojën për minimizimin e rrezikut nga shkatërrimi i rastësishëm ose joligjor, humbja, ndryshimi, zbulimi i paautorizuar ose qasja e paautorizuar në të dhënat personale që janë transferuar, ruajtur ose në ndonjë formë të përpunuara, si dhe ruajtjen e aftësisë për të siguruar konfidencialitet të vazhdueshëm, integritet, qasje dhe rezistencë të sistemit informatikë që përdoret për përpunimin e të dhënave personale dhe aftësisë për të pasur kthim të duhur të qasjes në të dhënat personale, në rast të incidentit fizik ose teknik, me qëllim që të sigurohet procesi i vazhdueshëm i punës.

### 3 Menaxhimi i rreziqeve

Për të përcaktuar se cilat masa teknike dhe organizative duhet të përcaktohen dhe zbatohen me qëllim të minimizimit të rrezikut nga shkatërrimi i rastësishëm ose joligjor, humbja, ndryshimi, zbulimi i paautorizuar ose qasja e paautorizuar në të dhënat personale që transferohen, ruhen ose në ndonjë formë përpunohen, me rëndësi është që fillimisht të përcaktohen / definojnë dhe të analizohen të gjitha proceset zyrtare në kuadër të organizatës që përpunon të dhëna personale dhe për të përcaktuar dhe vlerësuar rreziqet potenciale.

Procesi i menaxhimit të rreziqeve realizohet në disa faza:

- përcaktimi dhe hartimi i listës ose kontrollimi i proceseve zyrtare që përfshijnë përpunimin e të dhënave personale;
- vlerësimi i rreziqeve për secilin proces të përpunimit të të dhënave personale të përcaktuar gjatë fazës së parë;
- zbatimi dhe kontrollimi i masave të planifikuara që janë rezultat i vlerësimit dhe evalvimit të rreziqeve;
- realizimi i kontrollimeve periodike të sigurisë.

Nga ana tjetër, përcaktimi dhe hartimi i listës së proceseve zyrtare, të paktën i përfshin vendet ku të dhënat personale mund të përdoren si pjesë e aktivitetit zyrtar:

- pajisja harduerike (p.sh., serverët, laptopët, hard disqet dhe mediumet e tjera) në të cilat ruhen të dhënat personale në formatin digjital;
- pajisja softuerike (p.sh., sistemet operative dhe softuerët e zhvilluar për nevojat e kontrollorit) me të cilat kontrollori (ose përpunuesi) i përpunon të dhënat personale;
- kanalet komunikuese (p.sh., kablloptike, interneti, teknologjia e rrjetit pa tel, e a.q. wi-fi) përmes të cilave të dhënat personale kalojnë gjatë këtij procesi zyrtar;
- dokumentet në letër (p.sh., dokumentet e shtypura, kopjet) në të cilat ka të dhëna personale.





Gjatë vlerësimit të rreziqeve, kontrollorët dhe përpunuesit duhet të paktën, të bëjnë përpjekje maksimale për:

(a) identifikimin e ndikimit potencial dhe efektet ndaj të drejtave dhe lirive të personave fizikë nga kërcënimet e mundshme, respektivisht ngjarjet siç janë:

- qasja e paautorizuar në të dhënat personale;
  - ndryshimet e paplanifikuara të të dhënave personale;
- mospasja e përkohshme ose e plotë e qasjes në të dhënat personale.

(b) identifikimin e burimeve të rreziqeve që mund të jenë shkak për ngjarjen e padëshirueshme, duke marrë parasysh faktorët e brendshëm dhe të jashtëm njerëzorë (p.sh., administratori i sistemit informatikë, personi i autorizuar, sulmuesi i jashtëm, konkurrenti), si dhe faktorët e tjerë të brendshëm dhe të jashtëm jonjerëzorë (p.sh., vërshimet, materialet e dëmshme, zjarret, viruset);

(c) identifikimin e kërcënimeve potenciale që mund të paraqiten përmes medimeve në të cilat ruhen të dhënat (p.sh., hardueri, softueri, kanali komunikues, dokumentet në letër, etj.), e që mund të jenë:

- të përdorura në mënyrë joadekuate (p.sh., keqpërdorimi i autorizimeve, gabimet gjatë menaxhimit me të dhënat);
- të modifikuara (p.sh., softueri ose hardueri i robëruar – regjistrimi i shtypjeve në tastierë (keylogger), instalimi i softuerit me qëllim të keq, etj.);
- të humbura (p.sh., vjedhja ose humbja e pajisjes së lëvizshme siç janë laptopët dhe telefonat celularë ose medimet e transmetimit, siç janë memoriet e jashtme);
- të ndjekura (p.sh., gjeolokacioni i pajisjes);
- të dëmtuara (p.sh., vandalizmi, degradimi për shkak të përdorimit të zakonshëm);
- të mbingarkuar (p.sh., përmbushja e plotë e kapacitetit të mediumit për ruajtje, sulmi duke mos pasur qasje në shërbimet (denial of service attack), etj.);

(ç) përcaktimi i masave ekzistuese ose të planifikuara për zgjidhjen e rrezikut konkret (p.sh., kontrollimi i qasjes, kopjet rezervë / të sigurisë, përcjellja, siguria e hapësirave, kriptimi ose anonimizimi);

(d) vlerësimi i seriozitetit dhe probabilitetit të rreziqeve në aspekt të elementëve paraprakë të paraparë me vlerësimin e rreziqeve (p.sh., shkalla e rrezikut që mund të përdoret është si në vijim: rreziku i anashkaluar, i matur, i konsiderueshëm dhe maksimal);

(dh) nëse rreziku është i vlerësuar si i konsiderueshëm ose maksimal, bëhet përcaktimi i masave të tjera që mund të zbatohen për të minimizuar rrezikun.

Si rezultat i procesit për menaxhimin e rreziqeve, kontrollorët dhe përpunuesit duhet të përpilojnë dokumentacion që i mbulon këto aspekte me më shumë detaje:

- identifikimi, vlerësimi dhe klasifikimi i rreziqeve për proceset e përpunimit të të dhënave personale (analiza e rreziqeve);
- përshkrimi i përgjithshëm i masave teknike dhe organizative për të siguruar fshehtësinë dhe për të mbrojtur përpunimin e të dhënave që janë adekuate me rrezikun.

Pas vlerësimit të rreziqeve, kontrollorët dhe përpunuesit detyrimisht duhet të zbatojnë dhe kontrollojnë masat e planifikuara për t'u siguruar se ata edhe më tutje do t'i ruajnë rreziqet në nivelin minimal.

Kontrollorët dhe përpunuesit detyrimisht duhet të realizojnë kontrollime periodike të sigurisë së përpunimit për të cilat duhet të përpilojnë plane të veprimit, implementimin e të cilëve e ndjekin udhëheqësit e organizatës. Kontrollimet periodike të sigurisë së përpunimit duhet të





zbatohen për qëllimet e ruajtjes së hapit me zhvillimin teknologjik, për parandalimin e incidenteve të reja potenciale që bazohen në ndryshimet teknologjike dhe për zbatimin e masave mbrojtëse që mund të përgjigjen në mënyrë adekuate ndaj incidenteve të reja.

#### 4 Dokumentacioni për masat teknike dhe organizative

Si dokument kryesor për masat teknike dhe organizative, kontrollorët dhe përpunuesit hartojnë politikë për sistemin e mbrojtjes së të dhënave personale në organizatën e tyre. Në përputhje me proceset zyrtare dhe rreziqet e përcaktuara dhe të analizuar si pjesë e hapave të përcaktuar në kapitullin paraprak, dokumenti i tillë duhet t'i theksojë masat teknike dhe organizative që i zbaton kontrollori / përpunuesi.

Në bazë të politikës për sistemin e mbrojtjes së të dhënave personale, kontrollorët dhe përpunuesit miratojnë politika dhe procedura më të detajuara për çdo përpunim të të dhënave personale në kuadër të organizatës së tyre, e që përmbajnë përshkrime teknike dhe organizative për personat që kanë autorizime për qasjen në të dhënat personale dhe në sistemin informatikë dhe infrastrukturën. Ky dokument duhet të përfshijë më shumë detaje për:

- identifikimin, vlerësimin dhe klasifikimin e rreziqeve për proceset e përpunimit të të dhënave personale (analiza e rreziqeve);
- përshkrimin gjeneral të masave teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjes së përpunimit të të dhënave që përkasin me rrezikun;
- aktivitetet për trajnimin dhe krijimin e vetëdijes së menaxhmentit dhe punonjësve për rreziqet ndaj privatësisë dhe sigurisë në kuadër të kontrollorit;
- dizajnin, zhvillimin dhe mirëmbajtjen e softuerit për përpunimin e të dhënave, veçanërisht nga aspekti i teknikës dhe mbrojtjes së integruar të të dhënave personale (privacy by design and privacy by default);
- mënyrën e autentifikimit të personave të autorizuar në sistemin informatikë;
- mënyrën e kontrollimit të qasjes në sistemin informatikë;
- mënyrën e mbajtjes së evidencës për qasjen në sistemin informatikë (p.sh., qasja në sistemet operative, muri mbrojtës, softueri i dizajnuar special për datotekat, baza e të dhënave, softueri për menaxhimin e dokumenteve (DMS), softueri për menaxhimin e marrëdhënieve me klientët (CRM), etj.);
- mënyrën e menaxhimit të incidenteve (që e cenojnë konfidencialitetin, integritetin dhe qasjen në të dhënat);
- mënyrën e sigurimit të pajisjes së kontrollorit që shfrytëzohet për përpunimin e të dhënave;
- mënyrën e sigurimit të medimeve të transmetimit;
- mënyrën e sigurimit të rrjetit intern të kontrollorit (intranet);
- mënyrën e sigurimit të serverëve dhe ueb-faqeve të kontrollorit;
- mënyrën e mbajtjes dhe ruajtjes së dokumenteve në aplikacione / programe që përdoren për përpunimin e të dhënave;
- mënyrën e përpunimit të të dhënave të pseudonimizuara;
- mënyrën e përpunimit të të dhënave të kriptuara;
- detyrimet dhe përgjegjësitë e administratorit të sistemit informatikë dhe të personave të autorizuar, në lidhje me përdorimin e pajisjes informatike dhe komunikuese;





- mënyrën dhe proceset për informim, reagim ndaj incidenteve dhe kthimit të sistemit në gjendjen normale;
- mënyrën e krijimit, arkivimit dhe ruajtjes së kopjeve rezervë dhe mënyrën e kthimit të qasjes në të dhënat;
- mënyrën e shkatërrimit të dokumenteve, si dhe mënyrën e shkatërrimit, fshirjes dhe pastrimit të medimeve;
- sigurinë fizike;
- mënyrën e angazhimit dhe kontrollimit të subjekteve të jashtme (përpunuesve);
- dinamikën dhe mënyrën e realizimit të kontrollimeve periodike, si dhe proceseve të kontrollimit të brendshëm;
- masat e tjera që kontrollori i zbaton sipas analizës së zbatuar të rreziqeve.

## 5 Masat organizative

Pas definimit / përcaktimit dhe analizës së proceseve zyrtare gjatë të cilave përpunohen të dhënat personale dhe pas përcaktimit dhe analizës së rreziqeve potenciale për përpunimin, kontrollorët duhet t’i qasen sigurimit të masave organizative përkatëse për sigurinë e të dhënave personale që ata i përpunojnë në përputhje me dispozitat e LMDHP-së dhe Rregullores.

### 5.1 Niveli standard i masave organizative

Niveli standard i masave organizative që një organizatë duhet t’i zbatojë në bazë të proceseve të analizuara zyrtare që nënkuptojnë përpunimin e të dhënave personale edhe në bazë të rreziqeve potenciale të përcaktuara dhe të analizuara, është e rregulluar me nenet 30 deri 36 të Rregullores.

#### 5.1.1 Masat organizative për mbrojtjen e të dhënave personale (standardi minimal)

Neni 30 i Rregullores përcakton se kontrollorët (dhe përpunuesit) janë të detyruar që të zbatojnë standarde minimale të masave organizative, respektivisht:

##### 5.1.1.1 Përcaktimi i personave të autorizuar që kanë qasje në të dhënat personale

Varësisht nga organizata, respektivisht nga numri i punonjësve, si dhe varësisht nga proceset zyrtare në të cilat punojnë ose që janë për vendet e tyre të punës, nuk rekomandohet që punonjësit t’i dinë të dhënat personale (dhe jo vetëm) që mblidhen dhe përpunohen, ndërsa që nuk janë të lidhura me proceset zyrtare të vendit të tyre të punës.

Si masë për mbrojtjen e të dhënave personale nga qasja e paautorizuar në kuadër të organizatës, kontrollorët duhet të përcaktojnë se cilat vende të punës, në përputhje me proceset e punës që i realizojnë, kanë të drejtë në qasje, si dhe nivelin e qasjes dhe ndryshimit të të dhënave personale dhe vëllimit të të dhënave personale (dhe jo vetëm).

#### Shembuj:

*Një organizatë që merret me shitjen e pjesëve rezervë për automjete dhe ka selinë, magazinën dhe shitoren, të gjitha në lokacione të ndryshme. Një nga politikat zyrtare të organizatës është që të mundësojë dërgesën direkte të pjesës rezervë në adresën e shtëpisë së klientit, nëse pjesën e kanë dhe nëse bëhet fjalë për pjesë të madhe. Dërgesa e pjesëve të klienti bëhet nga magazina e organizatës.*





*Në shitore, blerësi dëshiron dërgesën e pjesëve të automjetit deri në adresën e tij të shtëpisë dhe shitësi i mbledh dhe i përpunon të dhënat e tij (emrin, adresën dhe numrin e telefonit) për t'i dërguar pjesët, si dhe e informon se dërgesa është nisur. Punonjësi në Departamentin e Resurseve Njerëzore nuk ka nevojë që të njoftohet me të dhënat personale të klientit, të cilat i ka mbledhur dhe i ka përpunuar shitësi në shitore, me qëllim që me sukses të realizohet procesi zyrtar. Nga ana tjetër, punonjësi i magazinës duhet të njoftohet me të dhënat personale të këtij blerësi që janë mbledhur dhe përpunuar nga shitësi që të mund t'ia dërgojë pjesët klientit në përputhje me procesin zyrtar të dërgesës së pjesëve. Departamenti i Resurseve Njerëzore merret me çështjet kadrovike të organizatës (përpunimin e të dhënave për punonjësit për të lidhur kontrata, parashtrimin e fletëparaqitjeve në institucionet e tjera, të përcaktuar me ligjet për marrëdhënie të punës në Republikën e Maqedonisë së Veriut). Për shkak të detyrimeve ligjore dhe natyrës së procesit zyrtar, punonjësit në Departamentin e Resurseve Njerëzore mbledhin dhe përpunojnë të dhëna për vendbanimin e punonjësve, anëtarëve të familjeve të tyre, gjendjen shëndetësore të punonjësve, etj. Punonjësit në magazinë ose punonjësit e shitores nuk kanë nevojë të dinë të dhënat personale të punonjësve të tjerë që i mbledh dhe përpunon Departamenti i Resurseve Njerëzore. Gjithashtu, udhëheqësi i Departamentit të Resurseve Njerëzore nuk duhet të ketë të drejta / autorizime për shtimin ose ndryshimin e të dhënave personale që të mund ta udhëheq Departamentin, ndërsa e drejta e vetme që duhet ta ketë është e drejta për kontrollimin e këtyre të dhënave.*

Varësisht nga madhësia e organizatës dhe resurset e disponueshme, kjo mund të rregullohet edhe përmes akteve / rregullave të brendshme që e përshkruajnë përpunimin konkret të të dhënave personale dhe i përcaktojnë autorizimet / të drejtat për përpunimin ose qasjen në të dhënat personale, aktet e brendshme të sistematizimit të vendeve të punës dhe përshkrimin e vendeve të punës, ku gjithashtu mund të theksohet se kush ka autorizime / të drejta për përpunimin ose qasjen në të dhënat personale, ose ajo mund të jetë pjesë e kontratës së punësimit dhe, siç është e rregulluar me nenin 31, paragrafët (4), (5) dhe (6) të Rregullores, përmes deklaratës së konfidencialitetit dhe mbrojtjes së përpunimit të të dhënave personale.

#### **Shembuj:**

*Departamenti i Resurseve Njerëzore i organizatës fillon procesin e punësimit të punonjësit të ri. Mes tjerash, kontrata e punësimit përfshin edhe nene ku, sipas vendit të punës, përcaktohet se personi do të punojë në kompjuter ku do të ketë qasje vetëm përmes emrit dhe fjalëkalimit, se do të ketë të drejtë të punojë me programe për përgatitjen e rrogave dhe me të drejtë që të shtojë, ndryshojë ose përpunojë të dhëna personale të punonjësve për qëllimet e pagesës së rrogave dhe kontributeve të detyrueshme. Gjithashtu, personi do të ketë qasje në internet përmes programit adekuat që të kryejë pagesën e rrogave në llogaritë bankare të nëpunësve dhe të bëjë pagesën e tatimeve dhe kontributeve adekuate.*

*Një organizatë dëshiron të instalojë sistem për video-mbikëqyrje në përputhje me dispozitat e LMDHP-së dhe Rregullores për mbajtjen e video-mbikëqyrjes, ku për këtë qëllim cakton një punonjës që do ta nënshkruaj DEKLARATËN për sigurinë e përpunimit të të dhënave*





*personale përmes sistemit për video-mbikëqyrje ku dakordohet dhe obligohet për t'i respektuar parimet e mbrojtjes së të dhënave personale, të zbatojë masa teknike dhe organizative për sigurinë dhe konfidencialitetin e përpunimit të të dhënave personale, për të përpunuar të dhënat personale në përputhje me udhëzimet e dhëna nga organizata e tij dhe të mos zbulojë kurrfarë të dhënash ose informacionesh të tjera personale ku ka qasje, respektivisht i ka zbuluar / do t'i zbulojë si pjesë e detyrave të tij të punës në organizatë, ndaj personave të tretë.*

Kur përcaktohen / konstatohen autorizimet me të drejtën e qasjes në të dhënat personale, kontrollorët janë të detyruar që të kenë kujdes që ato autorizime të dhëna ndaj një personi janë të shfuqizuara dhe do të sigurojnë se e drejta e qasjes është tërhequr menjëherë pas shfuqizimit të autorizimeve. Për këtë qëllim dhe në bazë të analizës së zbatuar të rreziqeve, kontrollorët i shqyrtojnë dhe përditësojnë autorizimet për qasjen në sistemin informatikë në intervale të rregullta, por të paktën një herë në çdo tre muaj.

#### **5.1.1.2 Rregullat organizative për qasjen në internet nga personat e autorizuar lidhur me shkarkimin dhe regjistrimin e dokumenteve që shkarkohen nga e-posta ose nga burimet e tjera**

Me rëndësi është që kontrollorët të krijojnë vetëdijen e punonjësve për përdorimin e sigurt të e-postës dhe përmbajtjeve në internet, ndërsa për këtë qëllim duhet të përcaktojnë rregulla organizative për qasjen në ueb-faqen e personave të autorizuar në lidhje me shkarkimin dhe regjistrimin e dokumenteve që merren nga e-posta ose burimet e tjera. Më poshtë janë dhënë disa prej rregullave bazike për përdorimin e sigurt të internetit:

- kur përdoret interneti, punonjësit duhet t'i vizitojnë vetëm ueb-faqet e nevojshme për realizimin e punës së tyre, respektivisht ueb-faqet zyrtare të kompanive ose institucioneve që kanë lidhje me punën e tyre;
- punonjësit nuk guxojnë që të përdorin pajisjen harduerike dhe internetin e organizatës për shkarkimin, kopjimin ose piratimin e programeve softuerike, filmave, muzikës dhe shënimeve elektronike që janë të mbrojtura me të drejtën autoriale, sekretet tregtare ose informacionet që kanë lidhje me pronësinë, shkresat e dedikuara për t'u hakuar nga ueb-faqet e paautorizuara, futjen e softuerëve me qëllim të keq në rrjetin e kompanisë ose që mund ta cenojnë sigurinë e sistemeve për komunikimin elektronik të organizatës;
- e-posta zyrtare duhet të përdoret vetëm për komunikimin zyrtar, jo edhe për qëllimet personale, për dërgimin ose publikimin e letrave-zinxhirë, për kërkesën e shërbimeve / mallrave, ose për reklamimet që nuk janë të lidhura me qëllimet ose aktivitetet zyrtare;
- punonjësit nuk duhet të hapin e-postë nga dërguesit e panjohur dhe/ose me përmbajtje të dyshimtë (p.sh., nëse marrin e-postë nga personi me emrin Piter Li nga [mickey.mouse@mikrosoft.cn](mailto:mickey.mouse@mikrosoft.cn) ose vetë adresa e e-postës nuk është bindëse dhe nuk duhet të hapet. Nëse përmbajtja e e-postës që vjen nga institucioni zyrtar, kërkon që pranuesi të hap linkun dhe të shënojë emrin dhe fjalëkalimin e përdoruesit në ueb-faqen e “institucionit zyrtar” për kontrollimin e të dhënave të përdoruesit ose për përditësimin e sistemit, e-posta e tillë nuk konsiderohet zyrtare, sepse asnjë institucion nuk kërkon që përdoruesit t'i kontrollojnë të dhënat e përdoruesit në atë mënyrë dhe për këtë punonjësi nuk duhet ta hap linkun. Në të dy rastet, e-posta duhet të fshihet ose të shënohet si “spam”).





### 5.1.1.3 Shkatërrimi i dokumenteve pas skadimit të afatit të tyre të ruajtjes

Edhe një masë për sigurinë informatike që përcaktohet me LMDHP-në ka të bëjë me faktin se të dhënat personale ruhen vetëm për afatin kohor kur janë të nevojshme për qëllimet e përpunimit.

Qëllimi i përcaktimit të kësaj mase, nga aspekti i sigurisë informatike është zvogëlimi i vëllimit të të dhënave personale në nivelin minimal, në rast të vjedhjes, përpunimit të paautorizuar ose të paligjshëm të të dhënave personale.

Për këto arsye, çdo organizatë duhet që vazhdimisht të mbajë llogari që nga sistemet e saj të përpunimit të të dhënave personale, t’i mënjanojë ato të dhëna për të cilat tashmë nuk ekziston qëllimi i përpunimit dhe për të cilat ka skaduar afati ligjor i ruajtjes.

#### Shembuj:

*Në shitoren e një kompanie që shet pjesë rezervë për automjete, klienti dëshiron që pjesët t’i dërgohen në adresën e tij të shtëpisë. Për këtë qëllim, nga klienti mblidhen të dhënat për emrin / mbiemrin, adresën e shtëpisë dhe numrin e telefonit dhe ato futen në programin kompjuterik të dedikuar për dërgesën e pjesëve dhe e informon klientin se procedura e dërgesës është në vijim. Pjesët i dërgohen klientit dhe ai padyshim e konfirmon porosinë në fletëdërgesën për t’i marrë pjesët e blera. Pas këtij akti, kompania nuk ka nevojë për ruajtjen e të dhënave të lartpërmendura të klientit në softuerin për përpunimin e faturave.*

*Një kompani siguron shërbime të telefonisë fikse dhe me konsumatorin lidh kontratë të re në çdo dy vjet. Kontrata dhe të dhënat personale duhet të përpunohen dhe të ruhen deri në arritjen e qëllimit / deri në realizimin e kontratës (plus periudhën e detyrueshme për kërkesa të mundshme financiare), deri sa faturat ruhen si dokumente të kontabilitetit në përputhje me rregullat për çështjet e kontabilitetit.*

Në afat të caktuar kohor, kompania duhet të shkatërrojë pajisjen që e përdor dhe për këtë gabim në punë ose parashkrim, ose nëse pajisja ka qenë e huazuar dhe afati i huazimit ka skaduar, ajo duhet të kthehet. Pajisja e tillë (veçanërisht kompjuterët dhe pajisjet e lëvizshme) ende përmbajnë të dhëna. Të dhënat që ruhen në formë digjitale duhet që të fshihen / shkatërrohen në mënyrë të sigurt përpara largimit të pajisjeve, si mbetje elektronike ose përpara dhurimit të saj kur një pjesë e pajisjes e ka ende të njëjtën vlerë të përdorimit.

Të dhënat në formë digjitale ruhen në pajisjet e magazinimit:

- disqe (hard-disqe, SSD-disqe, etj.) në kompjuterë, makina të kopjimit, pajisje për incizime që janë pjesë e sistemit të video-mbikëqyrjes, etj.;
- disqe të pajisjeve të lëvizshme, kartela të memorieve, SIM kartela, pajisje të lëvizshme;
- medime të transmetimit: disku shtesë, USB pajisje, kartela të memorieve, CD/DVD, shirita magnetike, etj.

Largimi i sigurt i të dhënave nga mediumi digjital mund të bëhet përmes:

- fshirjes së sigurt të mediumit për ruajtje;
- shkatërrimit fizik të mediumit për ruajtje;
- demagnetizimit.





Për fshirjen e sigurt të mediumit për ruajtje, nuk mjafton vetëm që të fshihen të dhënat ose formati i mediumit, sepse të dhënat e fshira ose të formatuara mund të kthehen me sukses. Fshirja e sigurt bëhet me programet e specializuara për atë qëllim. Mediumi i ruajtjes lidhet në kompjuter ku është instaluar programi për fshirjen e sigurt, më pas përmes lëshimit të programit dhe përzgjedhjes së mediumit, bëhet fshirja e sigurt e të dhënave. Procesi i fshirjes së sigurt merr shumë kohë dhe për këtë nuk konsiderohet opsion i standardizuar për fshirjen e datotekave dhe programeve në sistemet operative, sepse ajo dukshëm e zvogëlon shpejtësinë dhe funksionalitetin e kompjuterit.

Fshirja e sigurt në telefonat dhe tabletat inteligjentë bëhet përmes përzgjedhjes së opsionit për kthimin e cilësimeve fillestare të pajisjes.

Shkatërrimi fizik i mediumeve për ruajtje përfshin edhe copëtimin në pjesë më të vogla me qëllim që gjatë tentimit për lidhjen e mediumit, të pamundësohet kthimi i suksesshëm dhe qasja në të dhënat e ruajtura në ato mediume. P.sh., CD/DVD, si dhe dokumentet në letër që përmbajnë të dhëna, shkatërrohen me copëtues special për CD/DVD, me copëtues të letrës, pastaj hidhen. Disqet, disqet shtesë dhe kartelat e memorieve shkatërrohen në pjesë të vogla me copëtues.

Në treg ekzistojnë kompani të specializuara për fshirjen e sigurt të mediumeve dhe më pas lëshojnë certifikatë për shërbimin e tyre, me çka konfirmohet se mediumi ka qenë i fshirë në mënyrë të sigurt.

Përzgjedhja e metodave adekuate për fshirjen e sigurt ose shkatërrimin e të dhënave, varet edhe nga:

- vëllimi i të dhënave që janë të shënuara në medium;
- lloji të dhënave të shënuara në medium;
- lloji i mediumit ku ruhen të dhënat;
- gjendja e vetë mediumit.

Organizata duhet të formojë komisioni i cili harton procesverbal me të gjitha informacionet e nevojshme për identifikimin e plotë të dokumenteve dhe të kategorive të të dhënave personale që janë të shënuara në pajisjen që fshihet / shkatërrohet.

#### **5.1.1.4 Masat për sigurinë fizike të hapësirave dhe pajisjes informatike dhe të komunikimit në të cilën mblidhen, përpunohen dhe ruhen të dhënat personale**

Kur krijohen masat mbrojtëse, organizata duhet të mendojë për të inkuadruar masa adekuate fizike për mbrojtjen nga qasja e paautorizuar në hapësirat e saj dhe në pajisjen që e shfrytëzon.

Gjatë inkuadrimin të masave për mbrojtjen fizike, duhet të merren parasysh si në vijim:

- sigurimi i objektit nga qasja e paautorizuar jashtë orëve të punës së organizatës (p.sh., përmes instalimit të alarmeve kundër vjedhjes dhe përmes instalimit të sistemit për video-mbikëqyrje nëse vlerësimi i rrezikut tregon se ajo është e domosdoshme dhe e arsyeshme);
- kufizimi i qasjes në mobiljet e zyrës dhe hapësirat ku ruhen të dhënat personale dhe të dhënat e tjera konfidenciale (p.sh., hapësirat ku gjenden kompjuterët / serverët në të cilat ruhen të dhënat, hapësirat dhe sirtarët ku ruhen të dhënat në formë letre, etj.);





- kufizimi i qasjes në pajisjen ku ruhen të dhënat (serverët e kompjuterëve, disk-sistemet, disqet e jashtme) përmes vendosjes së tyre në mobiljen adekuate të zyrave (p.sh., raftet për serverë) ose në hapësirate ruajtura në mënyrë përkatëse, nga qasja e paautorizuar (p.sh., me shfrytëzimin e çelësave ose kartelave inteligjente);
- vendosja e pajisjeve të tjera (p.sh., internet-ruterë, ndërprerës të rrjeteve) në mobiljet adekuate të zyrave (p.sh., raftet për serverë) ose në hapësirat e ruajtura në mënyrë përkatëse, nga qasja e paautorizuar (p.sh., me shfrytëzimin e çelësave ose kartelave inteligjente);
- ndarja fizike e pajisjes së zyrave (kompjuterëve, printerëve, makinave të kopjimit, etj.) që shfrytëzohen për punë ndërvepruese me shfrytëzuesit e shërbimeve zyrtare nga vetë shfrytëzuesit e shërbimeve, ose të paktën, vështirësimi i qasjes në pajisjet dhe të dhënat (p.sh., ndërmjet shfrytëzuesve dhe vendit të punës) përmes vendosjes së sportelit që pengon përdoruesin për qasjen në pajisjet, printerët, makinat e kopjimit dhe mobiljet e zyrës ku ruhen të dhënat në formë letre, ose për t’u siguruar se ato nuk janë mjaft larg për të parandaluar përdoruesin që të ketë qasje në të dhënat, ndërsa monitori i kompjuterit të jetë i kthyer me anën e pasme drejt përdoruesit, etj.

#### **5.1.1.5 Harmonizimi me udhëzimet teknike për instalimin dhe funksionimin e pajisjes informatike dhe të komunikimit që përdoret për përpunimin e të dhënave personale**

Të gjitha punët e përcaktuara nga organizata përmes udhëzimeve teknike (ose ndonjë dokument tjetër) që kanë të bëjnë me masat për mbrojtjen e të dhënave personale, detyrimisht duhet të zbatohen dhe realizohen. Në të kundërtën, do të mbeten vetëm si “shkronja në letër”. Për këto arsye, është me rëndësi që organizata t’i zbatojë të gjitha masat për mbrojtjen e të dhënave personale, të përcaktuara me dokumentet interne për të minimizuar rrezikun nga shkatërrimi i rastësishëm ose joligjor, humbja, ndryshimi, zbulimi i autorizuar ose qasja e paautorizuar në të dhënat personale që transferohen, ruhen ose përpunohen, dhe për të ruajtur aftësinë për të siguruar konfidencialitet, integritet, qasje dhe aftësi të vazhdueshme për kthimin në kohë të qasjes dhe qasjen në të dhënat personale në rast të incidenteve fizike ose teknike për qëllimet e mundësimit të vazhdimësisë së proceseve të punës.

#### **5.1.2 Informimi dhe edukimi për mbrojtjen e të dhënave personale**

Faktori njeri është faktori më i rëndësishëm në procesin e zbatimit të masave të përcaktuara teknike dhe organizative për mbrojtjen e të dhënave personale, prandaj nëse të gjithë punonjësit pa marrë parasysh nivelin e tyre në hierarkinë e organizatës (nga drejtori / pronari deri te pastruesit), nuk janë të vetëdijshëm për rëndësinë e sigurisë informatike dhe përgjegjësisë së secilit person për mbrojtjen e të dhënave, atëherë masat e përcaktuara nuk kanë kurrfarë rëndësie.

Madje edhe kur vetëm një punonjës nuk është i vetëdijshëm për atë dhe i anashkalon masat e sigurisë informatike dhe mbrojtjes së të dhënave personale, ai/a jo e cenon tërë sistemin e organizatës dhe ekspozon ndaj vjedhjes potenciale, keqpërdorimit dhe humbjes së të dhënave personale dhe jo vetëm, që mblidhen dhe përpunohen si pjesë e aktivitetit zyrtar. Varësisht nga kategoria e të dhënave të “humbura” dhe vëllimit të tyre, pasojat mund të jenë





katastrofike të vetë organizatës dhe si rrjedhojë, për punonjësën që ka treguar këtë papërgjegjësi.

Ka rëndësi të jashtëzakonshme që të gjithë punonjësit të jenë të vetëdijshëm si në vijim:

- cilat të dhëna personale (dhe zyrtare) i përdorin dhe përpunojnë si pjesë e punës së tyre të përditshme;
- cilave kategori të të dhënave personale u përkasin ato (a janë të dhënat personale “të thjeshta”, të dhënat personale të fëmijëve, kategoritë e veçanta të të dhënave personale);
- ku gjenden këto të dhëna gjatë përpunimit të tyre;
- cilat janë rreziqet potenciale nga vjedhja, keqpërdorimi dhe humbja e këtyre të dhënave;
- si kjo mund të ndikojë negativisht ndaj organizatës ku punojnë, si dhe ndaj punonjësve në vijë të fundit;
- çfarë masash duhet të zbatohen për t’i mbrojtur këto të dhëna;
- nevoja për t’i zbatuar masat e rekomanduara dhe të përcaktuara për mbrojtje në bazë të përditshme, për të vendosur të gjitha rreziqet minimale nga qasja e paautorizuar dhe keqpërdorimet në pikën minimale.

Për këtë, që nga vetë angazhimi ose punësimi te kontrollori, si dhe veçanërisht përpara fillimit të karrierës së tyre në organizatë, të gjithë punonjësit detyrimisht duhet të njoftohen me rregullat për mbrojtjen e të dhënave personale, si dhe dokumentacionin e miratuar për masat teknike dhe organizative. Punonjësit ose personat e angazhuar nënshkruajnë deklaratë për fshehtësi dhe mbrojtje gjatë përpunimit të të dhënave personale, që ruhet si pjesë e dosjes së personit të punësuar ose të angazhuar.

Punonjësit që janë përgjegjës për menaxhimin e resurseve njerëzore te kontrollori e njoftojnë administratorin e sistemit informatikë për punësimin ose angazhimin e personave të autorizuar me të drejtë për qasjen në sistemin informatikë, për t’u siguruar se këta persona do të marrin emër dhe fjalëkalim për qasjen në pjesët e sistemit informatikë në bazë të autorizimeve të tyre për qasjen në të dhënat personale, si dhe për ndërprerjen e statusit të punës ose angazhimit të këtyre personave, për t’u siguruar se emrat dhe fjalëkalimet e tyre për qasje të fshihen, respektivisht të mbyllen për përdorim të mëtejshëm. Ajo duhet të bëhet edhe kur personi i punësuar ose i autorizuar e ndryshon vendin e punës ose kur merr më shumë ose më pak autorizime për shkak të ndryshimeve në dokumentacionin e miratuar për masat teknike dhe organizative.

Gjithashtu, organizata duhet të sigurojë informim dhe edukim të vazhdueshëm për udhëheqësit dhe personat e autorizuar në lidhje me detyrimet dhe përgjegjësitë e tyre të drejtpërdrejta për mbrojtjen e të dhënave personale.

### **5.1.3 Detyrimet dhe përgjegjësitë e administratorit të sistemit informatikë dhe të personave të autorizuar**

Personat e autorizuar, veçanërisht administratorët, nuk kanë vetëm të drejta, por kanë edhe detyrime dhe përgjegjësi në lidhje me sistemin informatikë. Kontrollori duhet t’i njoftojë administratorët dhe personat e autorizuar me dokumentacionin për masat teknike dhe organizative që kanë të bëjnë me realizimin e detyrimeve dhe përgjegjësitë të tyre. Në masë





të vogël, përgjegjësitë e tyre kanë të bëjnë me përdorimin e dokumenteve dhe pajisjes informatike dhe të komunikimit përmes zbatimit të masave të përcaktuara me Rregulloren dhe dokumentacionin intern me të cilin është rregulluar mbrojtja e të dhënave personale në organizatë dhe duhet të njoftohen edhe me detyrimet dhe përgjegjësitë e tyre në lidhje me sistemin informatikë (njësoj siç njoftohen me të drejtat e tyre).

Për shkak të autorizimeve të mëdha që i kanë në lidhje me sistemin informatikë të organizatës, administratorët e atyre sistemeve duhet të jenë nën mbikëqyrje dhe kontrollorët duhet t'i zbatojnë kontrollimet periodike të punës së administratorit të sistemit informatikë dhe të hartojnë raporte për ato kontrollime. Këto raporte duhet të përmbajnë informacione për parregullsitë e konstatuara (kur ka hapësirë) dhe propozim-masa për mënjanimin e tyre.

#### 5.1.4 Mbrojtja e të dhënave që ruhen në formë letre

Edhe krahas kompjuterëve bashkëkohorë dhe teknologjive moderne, subjektet e punës ende përdorin të dhëna që ruhen në formë të shkruar. Së këndejmi, rezultojnë edhe nevojat për përcaktimin e masave përkatëse për mbrojtjen e të dhënave në formë letre nga qasja e paautorizuar.

Siç ishte theksuar edhe paraprakisht, pa marrë parasysh nëse të dhënat ruhen në formë digjitale ose të letrës, nevojitet që të përcaktohet se cilat pozita të punës, në përputhje me proceset zyrtare që i realizojnë, kanë të drejtë të qasjes në spektrin e gjerë të të dhënave personale (dhe jo vetëm) që janë të nevojshme për realizimin e punës së tyre.

Megjithatë letrat janë medium fizik, ajo kërkon masa fizike për mbrojtje nga qasja e paautorizuar në të dhënat që ruhen në formë letre. Pas përdorimit, këto të dhëna detyrimisht duhet të ruhen në hapësirë përkatëse dhe në mobilje adekuate të zyrave (sirtarë, rafta, rafta të papërshkrueshëm nga zjarri, etj.) që janë të mbrojtura nga qasja e paautorizuar me përdorimin e çelësit ose ndonjë forme tjetër të sigurisë (p.sh., me kartelë me çip ose lexues të çipave), në vend që të ruhen në ambient të hapur (p.sh., në tavolinën e punës, në rafta të hapura, etj.).

Zbatimi i rregullit “byroja e pastër” është mënyrë që siguron se të gjitha dokumentet e rëndësishme, letrat konfidenciale, dosjet, librat, etj., hiqen nga byroja dhe mbyllin në hapësirë adekuate dhe në mobilje adekuate për zyrë, kur nuk përdoren ose kur punonjësi e lëshon vendin e tij të punës. Ajo është një nga strategjitë e larta që mund të përdoret për uljen e rrezikut ndaj sigurisë së të dhënave personale. Gjithashtu, në hapësirat e punës nuk duhet të ketë letra vetëngjitëse për shërbime dhe letra me informacione, siç janë emri dhe fjalëkalimi për përdorues ose numri i llogarive bankare, ndërsa kjo hapësirë duhet të lirohet nga dokumentet jothelbësore.

Pas arritjes së qëllimit dhe pas skadimit të detyrimit ligjor për ruajtjen e të dhënave në formë letre, këto dokumente duhet të shkatërrohen me makinë për prerjen e letrës. Për këtë qëllim, kontrollori formon komision që harton procesverbal me të gjitha informacionet e nevojshme për identifikimin e plotë të dokumenteve dhe kategorive të të dhënave personale të shënuara në to.





## 5.2 Niveli i lartë i masave organizative

Niveli i lartë i masave organizative është rregulluar me nenin 45 të Rregullores, ku thuhet se në rast të kopjimit ose shumimit të dokumenteve, ajo mund të bëhet vetëm nga ana e personave të autorizuar, që janë të përcaktuar nga kontrollori në procedurën ku detyrimisht përcaktohen masat dhe mënyra e kopjimit dhe shumimit të dokumenteve. Shkatërrimi i dokumenteve të kopjuara ose të shumuara duhet të bëhet në mënyrën që do të pamundësohet ripërtëritja / kthimi i mëtejme i të dhënave personale që janë shënuar. Edhe neni 46 i Rregullores ka të bëjë me nivelin e lartë të masave organizative, që përcakton se në rast të transferimit fizik të dokumenteve, kontrollori detyrimisht duhet të zbatojë masa për mbrojtjen e qasjes së paautorizuar ose menaxhimit me të dhënat personale të shënuara në ato dokumente.

## 6 Masat teknike

Pas përkufizimit / përcaktimit dhe analizës së proceseve të punës që nënkuptojnë përpunimin e të dhënave personale dhe pas identifikimit dhe analizës së rreziqeve potenciale për përpunim, si dhe pas përkufizimit të masave organizative përkatëse për sigurinë e të dhënave personale që përpunohen, kontrollorët duhet t'i zbatojnë të gjitha masat e përcaktuara me dokumentet e miratuara për masat teknike dhe organizative.

### 6.1 Niveli standard i masave teknike

Pas përkufizimit / përcaktimit dhe analizës së proceseve të punës që nënkuptojnë përpunimin e të dhënave personale dhe pas identifikimit dhe analizës së rreziqeve potenciale për përpunim, si dhe pas përkufizimit të masave organizative përkatëse për sigurinë e të dhënave personale që përpunohen, kontrollorët duhet t'i zbatojnë të gjitha masat e përcaktuara me dokumentet e miratuara për masat teknike dhe organizative.

Nenet 12 deri në 29 të Rregullores kanë të bëjnë me nivelin standard të masave teknike që duhet t'i zbatojë organizata në bazë të analizës së rreziqeve potenciale, si dhe të zbatojë masa teknike përkatëse për sigurinë e të dhënave personale që përpunohen.

#### 6.1.1 Zbatimi i masave teknike përkatëse për përmbushjen e dispozitave për autorizimet për qasje në të dhënat personale

Autorizimet për qasjen në të dhënat personale do të ishin vetëm një “shkronjë në letër” pa kurrfarë qëllimi praktik nëse nuk do të zbatoheshin masat e caktuara teknike që kanë të bëjnë me strukturën / objektet e organizatës, rrjetet, pajisjet harduerike dhe sigurinë e të dhënave në formë letre.

Autorizimet e punonjësve që u janë besuar si pjesë e pozitive të tyre të punës dhe të dhënat personale që i përpunojnë, duhet të zbatohen në të gjitha pjesët e sistemit informatikë të organizatës, e jo vetëm në pjesët ku punonjësit kanë autorizime. Ajo përfshin pajisjet harduerike (kompjuterët, printerët, skanerët, etj.), pajisjet e komunikimit, softuerin dhe hapësirat zyrtare / zyrat që kanë qëllime të përcaktuara. Këto të drejta për qasje duhet të shfuqizohen menjëherë pas skadimit të autorizimeve.





Në bazë të analizës së zbatuar të rreziqeve, kontrollorët i shqyrtojnë dhe i përditësojnë autorizimet për qasjen në sistemin informatikë për personat e autorizuar në intervale të rregullta kohore, por të paktën në çdo tre muaj, ku sipas udhëzimeve të kontrollorit, administratori i sistemit informatikë ndan, ndryshon ose shfuqizon autorizimet për qasjen në të dhënat personale dhe në pajisjet informatike dhe të komunikimit në përputhje me kriteret që i ka përcaktuar kontrollori.

Të gjithë punonjësit e autorizuar kanë qasje në sistemin informatikë dhe të komunikimit përmes identifikuesve unik, siç është emri dhe fjalëkalimi i përdoruesit, kartela inteligjente unike që u është dhënë, nënshkrimi digjital ose ndonjë metodë tjetër për autentifikim në përputhje me teknologjinë më të re që siguron identifikues unik vetëm me personin e autorizuar në kontekst të analizës së zbatuar të rreziqeve.

**Për shembull:**

Në përputhje me natyrën e punës së tij, administratori i sistemit ka qasje administrative në të gjithë kompjuterët dhe sistemin operativ në kuadër të organizatës përmes emrit dhe fjalëkalimit të përdoruesit, në dhomën e serverëve me kartelën inteligjente, në serverët dhe pajisjet e tjera informatike në dhomën e serverëve përmes fjalëkalimit administrativ për çdo server dhe për secilën pjesë të pajisjes së serverit, deri te pajisjet dhe rrjeti i komunikimit, sistemet operative të serverëve, softuerin zyrtar dhe bazat me të dhënat përmes fjalëkalimeve administrative për qëllimet e administrimit dhe rregullimit.

Për shkak të autorizimeve të tilla të mëdha dhe në bazë të analizës së zbatuar të rreziqeve, qasja e tillë mund të ndahet në disa administratorë, ku secili prej tyre ka mundësi që të qaset vetëm në pjesët e caktuara të sistemit informatikë të organizatës, për shembull, një administrator ka të drejtë të qasjes në pajisjet dhe rrjetet e komunikimit, një administrator tjetër ka të drejtë të qasjes në sistemin operativ të serverit, administratori i tretë ka të drejtë të qasjes në softuerin zyrtar dhe bazat e të dhënave të shënuara me softuerin, etj.

Nga ana tjetër, punonjësit e Departamentit të Kontabilitetit që i përlogarisin rrogat e punonjësve, kanë të drejtë të qasjes në kompjuterët e tyre të punës përmes emrit dhe fjalëkalimit të përdoruesit (ose përmes kartelës së tyre inteligjente), deri te softueri zyrtar i rrogave përmes emrit dhe fjalëkalimit të përdoruesit, por nuk kanë të drejtë të qasjes në, për shembull, kompjuterët dhe softueri zyrtar në Departamentin e Çështjeve të Kontabilitetit që përpunojnë të dhënat personale të klientëve.

Në bazë të analizës së zbatuar të rreziqeve për procesin konkret të punës, kontrollorët mund të përdorin kombinime të dy ose më shumë metodave për autentifikim, për disa ose për të gjithë personat e autorizuar (p.sh., emri dhe fjalëkalimi i përdoruesit në kombinim me një kartelë inteligjente).

Kontrollorët detyrimisht duhet të mbajnë evidencë për personat e autorizuar me të drejtat për qasjen në dokumentet dhe sistemin informatikë dhe detyrimisht duhet të krijojnë procedura të identifikimit dhe verifikimit të autorizimeve për qasje.

Në bazë të analizës së zbatuar të rreziqeve dhe në rastet kur verifikimi që bazohet në emrin dhe fjalëkalimin e përdoruesit (Rregullorja përcakton se fjalëkalimi duhet të krijohet me të paktën 8 karaktere dhe/ose shenja), kontrollorët detyrimisht duhet të zbatojnë rregulla që





garantojnë konfidencialitet dhe integritet në lidhje me informimin, ndarjen dhe ruajtjen e atyre informacioneve, ku fjalëkalimet duhet në mënyrë automatike të ndryshohen pas skadimit të afatit të definuar kohor që nuk guxon të jetë më i gjatë se tre muaj.

Duke marrë parasysh se fjalëkalimet janë metoda më e shpeshtë për mbrojtjen e sistemit informatikë dhe të komunikimit nga qasja e paautorizuar, të gjithë duhet të jenë të vetëdijshëm për disa rregulla që kanë të bëjnë me krijimin e fjalëkalimeve.

Një fjalëkalim detyrimisht duhet të përmbaj:

- 16 ose më shumë karaktere, sa më shumë - aq më mirë;
- shkronja të mëdha (ABCDEFGH, etj.);
- shkronja të vogla (abcdefgh, etj.);
- numra (34 123456);
- simbole (@ # \$% {} [] () / \ " ' , ; : < > ...).

Gjatë krijimit të fjalëkalimeve duhet të shmangen:

- fjalët e fjalive, veçanërisht në gjuhën angleze (airplane, laptop, RedSox, car, bicycle, computer, etj.);
- fjalëkalimet e përdorura më shpesh dhe të njohura në përgjithësi (password, default, admin, guest, etj.);
- të dhënat personale ose të dhënat e familjarëve (emri / mbiemri, data e lindjes, martesa, punësimi, etj., adresa e banimit, emrat e fëmijëve, familjarë të afërt, kanakare, emra të kompanisë, etj.) (Vlatko Markovski, Vlatko 14.02.1988., 14.02.1988, Ulica 111, 1000 Skopje, etj.);
- emri i përdoruesit (vlatko.markovski, vmarkovski, etj.),
- seritë e shkronjave, numrave dhe shenjave të njëjta (aaaaa, aaaa1111, aa11 ++, ..)
- përsëritja e fjalëve të njëjta (vlatkovlatko, plainplain, etj.);
- seritë e shkronjave dhe/ose të numrave në tastierë (qwertz, 123456, 1q2ë3e4r5t, etj.);
- të dhënat mirë të njohura identifikuese (p.sh., numri i amzës, numri i sigurimit shëndetësor, numri i letërnjoftimit, numri i tabelës së regjistrimit, adresa e vendit të punës, kati dhe numri i zyrës, etj. (SK-2324-BC, Boulevard Alexander the Great 29, etj.);
- fjalëkalimet keq të krijuara ose frazat keq të konvertuara (passëord123, passëord356, john1234, vlatko12345, p@ssw0rd, l0z1nk@).

Në internet ekzistojnë gjenerues që krijojnë fjalëkalime të forta në bazë të rregullave të lartpërmendura (shembull i një fjalëkalimi të gjeneruar: UZCQf] &} q {f4c + ct).

Fjalëkalimet e gjeneruara në këtë mënyrë (një seri e përzgjedhur me rastësinë e shkronjave, numrave dhe simboleve) janë të rënda për t'u mbajtur mend. Për këtë arsye, përdoruesit mund ta përdorin trukun e përzgjedhjes së frazës apo citatit për të gjeneruar fjalëkalim. Më pas shtohen simbolet dhe disa shkronja ndryshohen me numra ose simbole (për shembull, nga fraza „Fruit after rain“ mund të krijohet fjalëkalimi % Fru1t#@fT3r=r@1N+?). Ky fjalëkalim më lehtë mbahet mend në dallim nga ai që është përzgjedhur rastësisht nga seria e shkronjave, numrave dhe simboleve.

Fjalëkalimet e forta nuk duhet që detyrimisht të ndryshohen gjatë periudhave, në përputhje me rekomandimet e sigurisë të dhënë më lartë. Hulumtimet tregojnë se për shkak të ndryshimeve të shpeshta të fjalëkalimeve dhe nevojës së krijimit të fjalëkalimit unik për





qasjen në secilën pjesë të programit dhe për çdo program në veçanti, përdoruesit fillojnë të përdorin fjalëkalime më pak të sigurta ose e përdorin fjalëkalimin e njëjtë në disa pajisje dhe programe. Kur ekziston dyshimi se ai është kompromentuar nga përdoruesi i paautorizuar dhe mundëson qasjen e paautorizuar, fjalëkalimi i fortë i pajisjes ose programit duhet të ndryshohet.

Në epokën e sotme digjitale, të gjithë përdorim pajisje të ndryshme, sisteme digjitale informatike, shërbime digjitale, etj., dhe për këtë na duhet numër i caktuar i emrave dhe fjalëkalimeve për përdorues, për qasjen e autorizuar në secilën pjesë të pajisjes, në secilën pjesë të sistemit informatikë, në secilin shërbim digjital, etj., ose të paktën, na duhet fjalëkalimi unik. Për të mbajtur mend të gjitha fjalëkalimet, në internet mund të gjenden numër i madh programesh falas dhe komerciale për t’i menaxhuar fjalëkalimet që mund të instalohen në kompjuter ose në telefonin celular. Këto programe i ruajnë të gjitha emrat dhe fjalëkalimet në bazën e kriptuar me të dhënat për t’i mbrojtur nga qasja e paautorizuar dhe ato mund të jenë të dobishme për tërheqjen e lehtë të fjalëkalimeve kur ato na duhen.

Punonjësit nuk duhet t’i zbulojnë emrat dhe fjalëkalimet e tyre ndaj punonjësve të tjerë. Nëse ajo është e domosdoshme për shkaqe të jashtëzakonshme dhe të arsyeshme (p.sh., punonjësi është në pushim më të gjatë mjekësor dhe duhet të kemi qasje në kompjuter, programe dhe/ose e-postën e tij), pas përfundimit të asaj arsyeje, punonjësi duhet që menjëherë të ndryshojë fjalëkalimin e vjetër me fjalëkalim të ri.

### 6.1.2 Sigurimi i pajisjes që përdoret për përpunimin e të dhënave personale

Kontrollorët duhet t’i zbatojnë këto masa teknike për sigurimin e pajisjes që e përdorin për përpunimin e të dhënave personale:

- ndarja automatike e përdoruesit nga sistemi informatikë pas skadimit të afatit të caktuar pa aktivitet (jo më gjatë se 15 minuta);
- dalja automatike nga sistemi informatikë në rast të numrit të caktuar të tentimeve të pasuksesshme për hyrje që janë në kundërshtim me politikat e autentifikimit të kontrollorit; kontrollori duhet ta përcaktojë numrin e tentimeve të pasuksesshme për hyrje që është në përputhje me rrezikun dhe natyrën e proceseve të punës, në lidhje me përpunimin e të dhënave personale, por ai nuk guxon që të jetë më shumë se pesë tentime të njëpasnjëshme dhe të pasuksesshme;
- në rast të hyrjes së përsëritur pa sukses, personat e autorizuar duhet t’i nënshtrohen autentifikimit për t’u identifikuar nëse kanë ende autorizime për qasje në atë pjesë të sistemit informatikë ose u është ndaluar qasja për shkak të ndryshimeve në hapësirën e punës (ndryshimi i proceseve të punës, personi nuk ka më autorizime për qasje, etj.);
- instalimi i murit mbrojtës (firewall) në sistemin informatikë dhe cilësimet që lejojnë vetëm një numër të kufizuar të portave të autorizuara për komunikim për personat për të cilët është rreptësisht e domosdoshme që të kenë qasje të tillë, për të mundësuar funksionimin e drejtë të aplikacioneve të instaluara në stacionet e punës së kontrollorit;
- instalimi i programit antivirus i të gjithë kompjuterëve (stacioneve të punës ose serverëve) dhe politikës së definuar për përditësimin e rregullt të programit të antivirusit, përditësimin kritik të sistemit operativ dhe softuerit zyrtar, ku definohet se





të gjitha këto sisteme / programe duhet të përditësohen për t’i parandaluar mungesat kritike fabrike në intervalin që nuk është më i gjatë se një javë;

- konfigurimi paraprak i aplikacioneve për të siguruar përditësim automatik të sigurisë;
- kur mund të zbatohet, ruajtja e të dhënave të përdoruesit në serverët e kontrollorit duke bërë kopje të rregullta, ndërsa në rast të ruajtjes lokale të të dhënave (kur kontrollori nuk ka serverë për ruajtjen e të dhënave) dhe në bazë të analizës së zbatuar të rreziqeve, realizohet sinkronizimi i detyrueshëm i të dhënave ose masave për të bërë kopje rezervë;
- inkuadrimi i opsionit të kufizuar për të lidhur mediumet e transmetimit / eksterne (USB, kartela memorie, hard-disqe eksterne, etj.) në pjesët e sistemit informatikë që kanë rëndësi kritike;
- pamundësimi i funksionit për auto-lexim të mediumeve të transmetimit / eksterne (USB, kartela memorie, hard-disqe eksterne, etj.);
- marrja e pëlqimit paraprak nga konsumatorët e stacioneve të punës (personat e autorizuar) për përdorimin e mjeteve administrative nga largësia përpara intervenimit të stacioneve të tyre të punës, dhe me njoftim adekuat pas mbarimit të administrimit nga largësia (p.sh., duke treguar porosi në ekran se administrimi nga largësia ka përfunduar);
- lidhja e pajisjeve për furnizim të përhershëm me energji elektrike (pajisjet UPS) në pjesë të rëndësishme të sistemit informatikë (stacionet e punës, serverët, pjesët për ruajtjen e informacioneve, pajisjet e rrjetit);
- ndalimi për shkarkimin dhe instalimin e lirshëm të aplikacioneve nga interneti ose të paktën ndalimi për punë me aplikacionet e shkarkuara që nuk kanë burime të sigurta;
- kufizimi i përdorimit të aplikacioneve që kërkojnë të drejta për administrim vetëm nga ana e administratorëve;
- fshirja e të dhënave që ekzistojnë në stacionet e punës që duhet t’i ndahen një personi tjetër;
- në rast të stacioneve të komprometuara të punës, ndërmarrja e aktiviteteve për identifikimin e burimit dhe shenjat e hyrjes në sistemin informatikë të kontrollorit, me qëllim që të përcaktohet nëse ka dhe të tjera elemente të tij janë nën kërcënim;
- ndjekja e sigurt e pajisjes softuerike dhe harduerike që përdoret në sistemin informatikë të kontrollorit, përfshirë edhe ndjekjen e rregullt të qendrës nacionale për përgjigje ndaj incidenteve kompjuterike (MKD-CIRT) në lidhje me paralajmërimet dhe këshillat për rreziqet e pajisjes konkrete softuerike dhe harduerike;
- krijimi i vetëdijes së personave të autorizuar për çështjet që kërkojnë vëmendje të veçantë dhe sigurimin e informacioneve kontaktuese për personat që duhet t’i kontaktojnë në rast të incidentit ose dukurisë së ngjarjes së pazakonshme e cila ndikon në sistemin informatikë dhe të komunikimit të kontrollorit.

### 6.1.3 Mbajtja e evidencës për hyrjet në sistemin informatikë

Neni 15 i Rregullores e përmban këtë dispozitë:

„(1) Me qëllim që të sigurohet identifikimi i secilës qasje të paautorizuar (mashtuese) ose keqpërdorimit të të dhënave personale, si dhe të përcaktohet prejardhja e atyre incidenteve, kontrollori krijon dhe mban evidencë për secilën qasje / hyrje në sistemin informatikë (p.sh., nga sistemet operative, muri mbrojtës, softueri i dizajnuar special për përdorim si softueri i





datotekave, bazat e të dhënave, sistemi /softueri për menaxhimin e dokumenteve, sistemi / softueri për menaxhimin e klientëve, etj.)

(2) Evidenca nga paragrafi (1) i këtij neni në veçanti i përmban këto të dhëna: emrin / mbiemrin e personit të autorizuar, stacionin e punës prej ku qaset në sistemin informatikë, datën dhe kohën e qasjes, të dhënat personale ku kanë qasje, llojin e qasjeve me operacionet e ndërmarra në aspekt të përpunimit të të dhënave personale, shkresat e autentifikimit për qasjen, shkresat e qasjeve të paautorizuara, si dhe shkresat e refuzimit automatik nga ana e sistemit informatikë.

(3) Evidenca nga paragrafi (1) i këtij neni përmban edhe informacione për identifikimin e sistemit informatikë që është përdorur për tentime të jashtme për qasjen në funksionet operative ose të dhënat personale pa nivelin e nevojshëm të autorizimit.

(4) Operacionet që mundësojnë evidentimin e informacioneve nga paragrafët (2) dhe (3) të këtij neni, i kontrollon oficeri për mbrojtjen e të dhënave personale dhe/ose personi tjetër i autorizuar nga kontrollori që i posedon njohuritë dhe aftësitë e nevojshme, por nuk ka privilegje administrative dhe ato duhet të cilësohen / konfigurohen në mënyrë që pamundësojnë të dalin / deaktivizohen. Në aspekt të evidencës për qasje / hyrje, kontrollori mund të përdor edhe programe që gjenerojnë të dhëna të tilla në formë të thjeshtë dhe lehtë të lexueshme.

(5) Evidenca nga paragrafi (1) i këtij neni ruhet në afat prej të paktën pesë vjet.

(6) Oficeri për mbrojtjen e të dhënave personale e realizon kontrollimin nga paragrafët (2) dhe (3) të këtij neni, të paktën një herë në muaj dhe harton raporte për kontrollimin e realizuar dhe parregullsitë e konstatuara.

(7) Kontrollori i njofton personat e autorizuar për sistemin e krijuar për evidentimin e qasjes në sistemin informatikë.

(8) Kontrollori siguron mbrojtjen e sistemit të evidencës së qasjes në sistemin informatikë nga çfarëdo qasje e paautorizuar, veçanërisht nga ana e personave, aktiviteti i të cilëve evidentohet në shënimet e sistemit evidentues.

(9) Kontrollori siguron se personat e autorizuar për menaxhimin e sistemit për evidencë të qasjes në sistemin informatikë e njoftojnë udhëheqjen për të gjitha anomalitë ose incidentet e sigurisë, menjëherë ose më së voni në afat prej 12 orëve nga momenti i atij incidenti.

(10) Kontrollori e njofton Agjencinë për Mbrojtjen e të Dhënave Personale për secilin cenim të sigurisë së të dhënave personale, e nëse ekziston mundësia se ajo ngjarje do të rezultojë me rrezik të madh për të drejtat dhe liritë e personave fizikë, i informon edhe subjektet e të dhënave personale që ata të mund t'i kufizojnë pasojat e cenimit të sigurisë.

(11) Kontrollori i përdor informacionet e evidencës për qasjen në sistemin informatikë për qëllime të ndryshme nga qëllimi i përdorimit adekuat të sistemit informatikë (p.sh., përdorimi i shërbimeve për ndjekjen e orëve të punës së punonjësve, është keqpërdorim i sistemit informatikë).“

Edhe pse shumë pjesë të sistemit informatikë kanë shënime personale për qasje, ato shkresa jo gjithmonë i plotësojnë dispozitat nga neni 15 i Rregullores në raport me vëllimin e informacioneve që duhet të mblidhen në lidhje me evidencën për qasje (paragrafi (2) dhe paragrafi (3) nga neni 15). Gjithashtu, shumë pjesë të sistemit informatikë mund në mënyrë automatike të alarmojnë për anomalitë në aspektin e qasjes së paautorizuar në pjesët e sistemit informatikë (qasja potencialisht e paautorizuar). Neni 15 i Rregullores përcakton se personat e autorizuar e njoftojnë udhëheqësinë për të gjitha anomalitë ose incidentet e sigurisë menjëherë ose në afat prej 12 orëve nga momenti kur ka ndodhur ai incident.





Tërë kjo mund vështirë të përcaktohet nëse nuk zbatohet sistemi i ndjekjes së të gjitha qasjeve / hyrjeve në sistemin informatikë, t’i analizojë dhe t’i alarmojë personat e autorizuar për anomalitë në aspektin e qasjes së paautorizuar në pjesët e sistemit informatikë.

Për t’i plotësuar kërkesat e dhëna në nenin 15 të Rregullores, kontrollorët duhet të zbatojnë sistemin e sigurisë informatike dhe menaxhimit të ngjarjeve (SIEM). Ky sistem/softuer e kombinon menaxhimin e sigurisë informatike dhe menaxhimin e ngjarjeve të sigurisë për të siguruar analizën në kohë reale të alarmeve të sigurisë që i gjenerojnë programet dhe pajisjet harduerike të rrjetit. SIEM sistemi / softueri funksionon përmes mbledhjes së shkresave për qasjen dhe ngjarjen që i gjenerojnë programet e punës që i përdor organizata, pajisjet e sigurisë dhe sistemet e hostimit, dhe të gjitha i vendos në një vend, respektivisht në një platformë të centralizuar. SIEM sistemi / softueri mbledh informacione nga ngjarjet e antivirusit, shënimet e murit mbrojtës dhe nga lokacionet e tjera dhe ato i grupon sipas kategorive, për shembull, aktivitetet me qëllim të keq ose hyrja e pasuksesshme / suksesshme në sistem.

Kur ky sistem / softuer identifikon kërcënim duke ndjekur sigurinë e rrjetit, ai gjeneron alarm dhe e definon nivelin e kërcënimit në bazë të rregullave të përcaktuara paraprakisht. Për shembull, kur dikush tenton të hyjë në sistem përmes emrit/llogarisë më shumë se 10 herë në afat prej 10 minutave, ajo ngjarje duhet detyrimisht të shënohet si tentim për sulm të sistemit. Në këtë mënyrë, sistemi i detekton kërcënimet dhe menjëherë krijon alarme të sigurisë.

#### **6.1.4 Sigurimi i pajisjes së lëvizshme dhe medimeve të transmetimit**

Për shkak të faktit se mund të përdoren jashtë ambientit të sigurisë në kuadër të organizatës, pajisja e lëvizshme (laptopët / tabletat, printerët e lëvizshëm me memorie të brendshme, telefonat celularë, etj.) dhe medimet e transmetimit (disqet e jashtme, USB pajisjet, CD ROM, DVD, kartelat e memories, SIM kartelat, etj.) gjithnjë e më shumë dhe më shpesh janë të ekspozuar në qasjet e paautorizuara, humbjet ose vjedhjet dhe në këto situata, ata janë lëndë e prishjes potenciale të sigurisë së të dhënave personale.

Për këtë arsye, në bazë të analizës së zbatuar të rreziqeve dhe rezultateve nga analiza e tillë, dokumentacioni i brendshëm i kontrollorit duhet ta rregullojë mënyrën e përdorimit të asaj pajisjeje në kuadër të organizatës, me ç’rast duhet që ajo të përdoret vetëm nga ana e punonjësve me autorizime përkatëse dhe pas pëlqimit të marrë paraprakisht. Kur nuk e përdorin këtë pajisje, punonjësit me autorizime përkatëse duhet ta ruajnë në vend të sigurt ose në lokacion ku kanë qasje vetëm personat e autorizuar që janë të përcaktuar në dokumentet e brendshme të kontrollorit. Gjithashtu, personat e autorizuar duhet të njoftohen edhe me rregullat e brendshme në lidhje me përdorimin e këtyre pajisjeve. Për shembull, kur për shkak të natyrës së vendit të tyre të punës, në mënyrë shtesë gjatë punës në zyrë, punonjësit duhet të punojnë edhe jashtë organizatës, ata duhet të nënshkruajnë dokument për pranimin e pajisjes për të cilën kanë autorizim përkatës për përdorim edhe përpara përdorimit të saj, duhet të njoftohen me rregullat e përcaktuara të brendshme për përdorim adekuat të pajisjes, si dhe për masat që duhet t’i zbatojnë për ta mbrojtur atë. Kështu, kur nuk e përdorin pajisjen, punonjësit duhet ta ruajnë atë në vend ose lokacion të sigurt që përcaktohet nga kontrollori, siç janë zyrat dhe/ose raftet ku kanë qasje vetëm punonjësit e autorizuar.

Qasja në pajisjen e lëvizshme duhet të jetë e mbrojtur me emër dhe fjalëkalim të përdoruesit,





ndërsa nëse pajisja nuk e ka atë opsjon, edhe me program me disa faktorë të autentifikimit. Pajisja e lëvizshme për ruajtjen e të dhënave (disqet) dhe mediumet e transmetimit (disqet e jashtme, CD ROM, DVD, kartela memorie, SIM kartela) duhet të kriptohen me masa të forta të kriptimit që në rast të humbjes ose vjedhjes, do të garantojnë se të dhënat që ruhen aty të mos jenë të lexueshme dhe të kenë qasje pa autorizim. Nëse sistemi operativ i pajisjes së lëvizshme ofron kriptimin e disqeve, kriptimi mund të bëhet përmes atij opsioni, në të kundërtën, për atë qëllim duhet të përdoren programe softuerike kredibile të dizajnuara për kriptimin e disqeve për ruajtjen e të dhënave dhe medimeve të transmetimit me zbatimin e rregullit për krijimin e fjalëkalimeve të forta. Këto programe duhet të përdorin algoritme të dëshmuara për kriptim, siç janë AES, Serpent, Tëofish, Camellia, Kuznyechik ose kombinimet kaskade të tyre për siguri plotësuese me hash-funksionet e dëshmuara për kriptim SHA-256, SHA-512, RIPEMD-160, etj. Kur ekziston si opsjon, rekomandohet zbatimi i funksionit për fshirjen e tërë përmbajtjes së medimeve për ruajtjen e të dhënave sipas numrit të caktuar të tentimeve të pasuksesshme për qasjen e autorizuar lidhur me qasjen në pajisjet e lëvizshme (hyrja dhe fjalëkalimi) ose në aspekt të dekriptimit të mediumit.

Kur planifikohet përdorimi i shërbimeve kompjuterike në retë (cloud services) për ruajtjen e të dhënave, kontrollorët fillimisht duhet të përcaktojnë nëse ofruesi i atyre shërbimeve, zbatohet mbrojtja adekuate e të dhënave personale përmes realizimit të analizave të rreziqeve dhe duhet t'i zbatojë të gjitha masat organizative të përcaktuara me LMDHP-në dhe masat që duhet të zbatohen për mbrojtjen e të dhënave personale, etj.)

Ruajtja e të dhënave në pajisjen e lëvizshme dhe mediumet e transmetimit duhet të kufizohet vetëm në vëllimin minimal të të dhënave të nevojshme për realizimin përkatës të detyrave të punës.

Masa shtesë që mund të zbatohet ka të bëjë me vendosjen e filtrave për privatësinë e ekraneve të pajisjeve të lëvizshme kur ajo përdoret në vendet publike ose të përdoret pajisja e lëvizshme që tashmë ka filtra të integruar të privatësisë.

Masa tjetër plotësuese përfshin kriptimin e pajisjeve për ruajtjen e të dhënave, por edhe kriptimin e të dhënave që ruhen në pajisjen e lëvizshme dhe/ose pajisjet e transmetimit. Edhe një masë plotësuese e rekomanduar ka të bëjë me konfigurimin e mbylljes automatike të pajisjeve të lëvizshme pas disa minutave pasivitet, si dhe pastrimit të të dhënave të mbledhura menjëherë pasi të jenë transmetuar në sistemin informatikë të kontrollorit.

#### 6.1.5 Sigurimi i rrjetit intern (intranet)

Varësisht nga madhësia e organizatës dhe numrit të pajisjeve të punës (kompjuterët, laptopët, makinat e kopjimit të lidhura me rrjet, etj.) dhe proceset e punës, pajisja e tillë duhet të lidhet në kuadër të rrjetit lokal. Për lidhjen e pajisjes përdoren ndërprerës të rrjetit.

Edhe ndërprerësit e rrjetit detyrimisht duhet të jenë të mbrojtur fizikisht nga qasja e paautorizuar me çka do të vendosen në hapësirën interne të organizatës, në rafte për rrjetin ose mobilje të tjera të siguruar me çelës, me çka në ato rafte do të kenë qasje fizike vetëm personat e autorizuar.

Sipas mundësisë, rekomandohet përdorimi i ndërprerësve të rrjetit që mund të konfigurohen. Këta ndërprerës lejojnë cilësimin e masave plotësuese të sigurisë, siç janë deaktivizimi i





vendeve për kabllot e rrjetit përmes të cilave lidhen pajisjet deri në momentin kur ato duhet të vihen në përdorim.

Gjithashtu, këta ndërprerës lejojnë cilësime që përcaktojnë se cilat pajisje mund të lidhen midis vete dhe cilat pajisje kanë të drejtë për lidhje interne. Nëse organizata nuk ka ndërprerës të tillë të rrjetit, lidhja interne mund të vendoset përmes murit mbrojtës dhe/ose ruterëve internë.

Kontrollorët sigurojnë mbrojtjen e rrjetit të tyre intern duke përdorur vetëm ato funksione të domosdoshme të rrjetit për përpunimin e të dhënave personale, veçanërisht përmes kufizimit të qasjes në brendësi, si dhe përmes bllokimit të shërbimeve jothelbësore (p.sh., telefonisë së brendshme (VoIP), lidhjet “pikë për pikë” (peer to peer), etj.).

Ruteri intern është pajisje e cila mundëson lidhjen e sistemit informatikë lokal intern dhe ai krijohet nga ofruesi i shërbimeve interne që e përdor organizata, si pjesë e pajisjes për qasje interne. Meqë ky ruter është drejtpërdrejt i lidhur në brendësi dhe paraqet lidhje ndërmjet pajisjes digjitale të organizatës dhe internes, ka rëndësi esenciale që ai të ketë cilësime / rregullime përkatëse për të siguruar mbrojtjen kualitative nga qasja e paautorizuar.

Ofruesit e shërbimeve interne sigurojnë ruterë me emër dhe fjalëkalim të përcaktuar paraprakisht për administrimin ose konfigurimin e cilësimeve të ruterit intern. Varësisht nga modeli dhe marka e ruterit intern, këto informacione dihen mirë, prandaj edhe duhet detyrimisht të ndryshohen për të penguar qasjen e lehtë nga ana e hakerëve që mund t'i përdorin këto informacione për administrimin e ruterit intern dhe për të hyrë në sistemin e punës së kontrollorit përmes internes për të realizuar aktivitetet e mëtejshme me qëllim të keq. Për këtë arsye, kontrollorët duhet ta ndryshojnë emrin dhe fjalëkalimin e përcaktuar paraprakisht të kësaj pajisjeje me emër dhe fjalëkalim unik që janë të njohur vetëm për punonjësit e autorizuar për administrimin e ruterëve intern.

Për të funksionuar në mënyrë adekuate, secili ruter intern përmban program (firmver) që e mundëson funksionimin. Prodhuesit e ruterëve intern vazhdimisht publikojnë versione të reja të firmverëve pas zbulimit të gabimeve gjatë punës së programit dhe rreziqet e sigurisë sipas cilësimeve të programit. Për këtë arsye, kontrollorët duhet që rregullisht t'i përditësojnë ruterët me versionin më të ri zyrtar të publikuar nga prodhuesi i modelit dhe markës së ruterit intern që ata e përdorin.

Rekomandohet që tërë pajisja e sistemit informatikë e organizatës që duhet të lidhet në interne përmes ruterit të lidhet përmes kabllave të rrjetit. Pajisjet e caktuara, si p.sh., telefonët dhe tabletët inteligjentë, nuk kanë mundësi për t'u lidhur përmes kabllave, andaj ajo detyrimisht duhet të lidhet përmes rrjetit patel të ruterit intern (a.q., rrjeti wi-fi). Për këtë qëllim, në cilësimet e ruterit definohet se fjalëkalimi për lidhje patel duke shfrytëzuar protokollin e sigurisë WPA2-PSK dhe krijimin e fjalëkalimit të ri sipas rekomandimeve për fjalëkalime të forta.

Opsioni WPS i dedikohet lidhjes më të lehtë patel të pajisjeve me ruterin intern duke klikuar butonin në ruter ose përmes shënimit të PIN-it numerik. Hakerët lehtë mund ta zbulojnë PIN-in për lidhje patel përmes EPS, prandaj ky opsion duhet të pamundësohet / deaktivizohet.





Modelet më të reja të ruterëve intern kanë opsion që mundëson qasjen nga largësia deri te ruteri përmes internes (a.sh. qasja e jashtme). Nëse nuk ka nevojë për qasjen administrative në ruterin intern nga jashtë, rekomandohet që edhe ky opsion të pamundësohet / deaktivizohet për arsye sigurie.

Gjithashtu, modelet më të reja të ruterëve intern, përfshijnë opsionin për hyrjen universale dhe për lexim (UPnP), dedikuar për lidhjen e lehtë të pajisjeve moderne të amvisërisë (p.sh., TV pajisjeve, konzolave për lojëra, etj.) për t’i shmangur cilësimet përmes dritareve me qëllim që ato të lidhen në ruter. Nëse ky opsion është i lidhur/mundësuar, viruse të ndryshme mund të kenë qasje administrative në ruterin intern, prandaj ajo duhet të pamundësohet / deaktivizohet.

Qasja përmes ruterit intern përmes filtrimit të MAC-adresave të pajisjes (kompjuterit, telefonit celular, tabletit, etj.) mund të kufizohet me cilësime përkatëse të masave të sigurisë. MAC-adresa është pjesë e pajisjes që mundëson lidhjen në ndonjë rrjet dhe zakonisht pasqyrohet në njërin prej cilësimeve të rrjetit të pajisjes në formën e 6 çifteve të shifrave të ndara me vizë (01-23-45-67-89-ab) ose në formë të 6 çifteve të shifrave të ndara me nga dy pika (01: 23: 45: 67: 89: ab). Shënimi i MAC-adresës në pajisjen që ka qasje të lejuar në ruterin intern e pamundëson qasjen në të gjitha pajisjet e tjera që nuk janë të shënuara në atë listë.

Vëmendje e veçantë duhet t’i kushtohet edhe mundësimin të qasjes në ruterin intern dhe me të të pamundësohet qasja në interne për punonjësit që nuk kanë nevojë për të përdorur interne si pjesë e proceseve të tyre të punës, si dhe për palë të treta (partnerë zyrtarë, klientë, përdorues, etj.) Nëse për qëllimet e rritjes së nivelit të shërbimeve, organizata dëshiron të sigurojë qasje interne për të gjithë punonjësit dhe për palët e treta përmes rrjetit ëi-fi, atëherë ai rrjet duhet të ndahet, nuk duhet të lejohet qasja në rrjetin intern zyrtar, ndërsa ruteri intern duhet të ketë opsion që atë ta bëjë përmes ruterit tjetër apo murit mbrojtës.

Ruteri intern duhet të jetë i mbrojtur fizikisht nga qasja e paautorizuar. Rekomandohet që ruteri të vendoset në hapësirë të mbyllur ose pajisje të zyrave të siguruara me çelës, ku kanë qasje vetëm personat e autorizuar të organizatës.

Nëse ka nevojë për qasje nga largësia në sistemin e rrjetit intern informatikë, ajo lidhje duhet të realizohet përmes lidhjes VPN duke përdorur protokolle të dëshmuara dhe të sigurt dhe algoritme për kriptim (p.sh. L2TP dhe IPSec, SSTP, etj.) dhe me autentifikimin e detyrueshëm për personat e autorizuar (p.sh., kartela inteligjente, pajisje për gjenerimin e fjalëkalimeve për një përdorim – OTP, etj.)

Nëse ka nevojë për mirëmbajtje nga largësia, atëherë duhet të sigurohet se interfejsi ose cilësimet e sistemit për administrim, nuk janë drejtpërdrejtë të qasshme përmes internes. Ajo mund të bëhet vetëm përmes lidhjes VPN , siç u shpjegua më lartë.

Komunikacioni përmes rrjetit duhet të kufizohet përmes filtrimit të komunikimeve të hyrjes / të daljes së pajisjes me mure mbrojtëse, proksi serverë, etj. (p.sh. nëse organizata ka ueb-server që është pjesë e infrastrukturës së tij, atëherë ueb-serveri përdor HTTPS dhe për këtë duhet të sigurohet se komunikimet e hyrjes në atë server realizohen vetëm përmes portit 443 dhe se portet e tjera janë bllokuar).





Për rregullimin e të gjitha këtyre cilësimeve nevojitet njohja e protokolleve të rrjetit dhe porteve të rrjetit, prandaj nëse organizata nuk ka punonjës me njohuri të tilla specifike, duhet të bashkëpunojë me persona të jashtëm që zbatojnë masa adekuate për sigurinë e të dhënave në përputhje me rregullat për mbrojtjen e të dhënave personale.

#### 6.1.6 Sigurimi i serverëve

Duke marrë parasysh se serverët përpunojnë (dhe ruajnë) një numër të madh të të dhënave, ato duhet të kenë prioritet në aspekt të zbatimit të masave teknike dhe organizative përkatëse.

Rregullorja përcakton se, si standard minimal, kontrollorët duhet t'i zbatojnë këto masa:

- Kufizimin e rreptë të qasjes në serverë, mjetet e serverëve dhe panelet administruese vetëm për punonjësit e autorizuar (administratorët) që janë përcaktuar me dokumentet interne që i rregullojnë autorizimet për qasje në serverët. Kontrollorët duhet të kenë parasysh se punonjësit e autorizuar duhet të posedojnë njohuri adekuate për administrimin e softuerëve. Në rast kur, për shkak të mungesës së resurseve njerëzore adekuate, kontrollori duhet të angazhojë bashkëpunëtorë të jashtëm, atëherë duhet t'i zbatojë të gjitha masat e sigurisë të përcaktuara me LMDHP-në dhe Rregulloren (p.sh., administratori i rrjetit intern duhet të ketë autorizim për qasje dhe administrim jo vetëm të pjesëve të serverëve që i administrojnë përdoruesit e rrjetit dhe autorizimet e tyre, si dhe nuk duhet të kenë qasjen në bazat me të dhëna që ruhen në serverët ose përmbajtjen e pajisjeve për ruajtjen e të dhënave).
- Autorizimet për qasjen e punonjësve që nuk janë administratorë të sistemit informatikë duhet të kufizohen vetëm për qasjen e pjesëve joadministrative të serverëve, në përputhje me dokumentet interne të kontrollorit dhe natyrës së punës që e realizojnë këta punonjës (p.sh., kontrollori ka miratuar politikën se të gjithë punonjësit duhet t'i ruajnë dokumentet digjitale në folder me të dhënat e serverit, ku secili i punësuar ka folderin e tij dhe autorizimet për qasje / lexim / rregullim vetëm të dokumenteve në folderin e tij/saj dhe nuk ka autorizime për qasjen në folderët e tjerë në server, ndërsa udhëheqësit-përveç autorizimeve për qasjen në folderët e tyre në serverë - kanë autorizime edhe për kontrollimin e dokumenteve të folderëve të punonjësve të Departamentit të tij/saj).
- Për shkak të autorizimeve të mëdha që i kanë administratorët e sistemit në aspekt të sistemit informatikë, kontrollori duhet të miratojë politikë të veçantë për krijimin e fjalëkalimeve për administratorët që është më ndryshe se politika e krijimit të fjalëkalimeve për punonjësit që nuk kanë privilegje administrative (p.sh, autentifikimi me disa faktorë për llogaritë / urdhëresat administrative, ndryshimi i fjalëkalimit pas largimit nga vendi i punës së ndonjë administratori, etj.).
- Për shkak të rrezikut të shtuar nga qasja e paautorizuar në server, krahasuar me rrezikun e qasjes së paautorizuar të stacioneve të punës, në bazë të analizës së zbatuar të rreziqeve, të gjitha përditësimet e serverit (p.sh., përditësimi i sistemit operativ, sistemi për hyrje-dalje – BIOS, serveri me bazën e të dhënave, programet e punës, etj.) duhet të bëhen në intervale të rregullta që nuk janë më të gjata se një javë. Për arritjen e këtij qëllimi, sipas mundësisë, duhet të zbatohet përditësimi





automatik (p.sh., përditësimi automatik i sistemit operativ, serveri me bazën e të dhënave, etj.).

- Sipas analizës së zbatuar të rreziqeve, kontrollorët duhet të krijojnë kopje rezervë të serverit në intervale të rregullta. Gjithashtu, kontrollorët duhet të bëjnë kontrollime të rregullta të funksionit për kthimin e sistemit për të përcaktuar nëse përmbajtja e serverit mund të kthehet në gjendje normale (pa humbur të dhëna) në rast të incidentit.
- Nëse serveri përdoret për shkëmbimin online të të dhënave, si standard minimal, ai komunikim duhet të kriptohet me protokoll që është i dizajnuar për komunikime të sigurta përmes rrjetit kompjuterik (p.sh., TLS1..3). Gjithashtu, kontrollori duhet të bëjë kontrollime vjetore të konfigurimit të protokollit kriptografik për të parë nëse ato janë cilësuar / vendosur si duhet ose gjithmonë kur ka informacione me qasje publike për rreziqet më të mëdha të sigurisë në protokollin konkret, me qëllim që të sigurohet efektiviteti i mbrojtjes.

Kur serveri përdoret për ruajtjen e bazave me të dhëna, për qëllime të administrimit të sigurt të bazave me të dhëna, si standard minimal, kontrollori duhet të përdor profile të paprofesionalizuara për qasjen në to dhe krijimin e emrave konkretë për përdorues për çdo aplikacion / program. Një masë tjetër që duhet të zbatohet si standard minimal në aspekt të serverëve me bazat e të dhënave ka të bëjë me mbrojtjen adekuate nga sulmet duke injektuar kode në bazat e të dhënave (SQL injection).

### 6.1.7 Sigurimi i ueb-faqeve

Kur përdorin ueb-faqe, kontrollorët duhet të sigurojnë që ato janë të mbrojtura nga qasja e paautorizuar, veçanërisht në rastin e ueb-faqeve që përpunojnë të dhëna personale (p.sh. biskota, autorizimet për qasje në pjesët e ueb-faqes që imponojnë autorizime të tilla, plotësimin e formularëve që përpunojnë të dhëna personale, etj.).

Për t'i mbrojtur ueb-faqet e tyre, kontrollorët duhet t'i ndërmarrin hapat e mëposhtëm:

#### 1. Mbajtja e llogarisë që softueri dhe të gjitha bashkëngjitjet janë përditësuar

Përditësimet janë me rëndësi jetike për shëndetin dhe sigurinë e një ueb-faqeje, sepse nëse softueri dhe bashkëngjitjet nuk janë të përditësuar, atëherë ueb-faqja nuk është e sigurt. Versionet e përditësuar shpesh përfshijnë përf forcime të sigurisë dhe përmirësime të cenueshmërive të programeve të tilla. Për këtë arsye, kontrollorët duhet të kontrollojnë disponueshmërinë e versioneve të përditësuar dhe të shtojnë bashkëngjitje me njoftimin për versionet e reja / të përditësuar. Disa platforma lejojnë përditësimin automatik dhe ky është edhe një opsion që mundëson sigurinë e ueb-faqes.

#### 2. Shtimi i certifikatave për HTTPS dhe SSL

Për të siguruar që ueb-faqja është e sigurt, veçanërisht kur vizitorëve u kërkohet të regjistrohen ose të identifikohen ose kur bëjnë transaksione, është e nevojshme që ueb-faqja të ketë URL të sigurt (përkatësisht link në ueb-faqen, për shembull: <https://mywebsite.mk>) dhe lidhja të jetë e kriptuar. Pse duhet të përdoret protokollin HTTPS në vend të protokollit HTTP? Pra, HTTPS (Hypertext Transfer Protocol Secure) është protokoll që përdoret për të garantuar sigurinë online. Ai parandalon përgjimin e komunikimit dhe ndërprerjet në transmetimin e përmbajtjes.





Për të siguruar komunikim të sigurt në internet, ueb-faqja duhet të ketë certifikatë SSL. SSL (Secure Sockets Layer) i kripton informacionet e transmetuara në internet nga ueb-faqja deri në pajisjet e përdoruesve me qëllim që të parandalojë leximin e tyre nga palët e treta gjatë transmetimit. Gjithashtu, kjo certifikatë pamundëson qasjen në të dhënat pa autorizimin përkatës.

**3. Ndalimi i portave të komunikimit në internet që nuk janë të domosdoshme**

Portat e komunikimit duhet të kufizohen vetëm në ato që rreptësisht janë të nevojshme për funksionimin përkatës të ueb-faqes. Për shembull, nëse ueb-serveri pranon lidhje vetëm përmes protokollit HTTPS, komunikacioni përmes rrjetit IP duhet të lejohet vetëm përmes portit 443, ndërsa të gjitha portet e tjera duhet të bllokohen.

**4. Zgjedhja e fjalëkalimit të fortë**

Sistemi i Menaxhimit të Përmbajtjes (CMS) imponon hyrjen dhe për këtë qëllim duhet zgjedhur fjalëkalim i fortë në përputhje me dispozitat e dhëna në nenin 11 të Rregullores, prandaj rekomandohet krijimi i fjalëkalimit të fortë, siç shpjegohet në këtë udhërrëfyes. Gjithashtu, fjalëkalimet nuk duhet të ruhen në kornizat e regjistrave të ueb-faqes.

**5. Përdorimi i ofruesit të sigurt të shërbimeve për hostimin e ueb-faqeve**

Për të ilustruar se çfarë është emri i ueb-domenit dhe çfarë është ueb-hosti, respektivisht ueb-nikoqiri, domenin e ueb-faqes suaj, konsiderojeni si adresën e rrugës, ndërsa ueb-hostin si parcelën ku ueb-faqja juaj ekziston në hapësirën online. Ashtu si parcela kontrollohet për të siguruar që ajo është mjaftueshëm e sigurt për shtëpinë tuaj, ashtu duhet të kontrollohet edhe ofruesi potencial i shërbimeve të ueb-hostimit për të parë nëse ai është i vërteti për nevojat e kontrollorit. Kur zgjidhni ofrues të sigurt të shërbimeve të tilla, duhet të merren parasysh / shqyrtohen si në vijim:

- A ofron ofruesi i shërbimeve Protokoll të Transmetimit të Sigurt të Datotekave (SFTP)?
- A është çaktivizuar opsioni për të përdorur Protokollin e Transmetimit të Datotekave (FTP) nga përdoruesi i panjohur?
- A përdor ofruesi i shërbimeve Rutkit Skaner (Rootkit Scanner)?
- A ofron ofruesi i shërbimeve hartimin e kopjes rezervë të datotekave?

**6. Përcaktimi i autorizimeve për administrimin dhe evidencën e qasjes nga përdoruesit**

Siç rregullohet në nenin 11 të Rregullores, si pjesë e dokumentacionit intern, kontrollori përcakton se kush ka të drejtë të administrojë ueb-faqen. Gjithashtu, në përputhje me nenin 15 të Rregullores, kontrollori mban evidencë për qasjen në ueb-faqen nga përdoruesit. Evidenca e tillë duhet t'i përmbajnë informacionet e mëposhtme: emrin / mbiemrin e personit të autorizuar, stacionet e punës nga të cilat është bërë qasja në sistemin informatikë, datën dhe orën e qasjes, të dhënat personale në të cilat ka pasur qasje, llojin e qasjes dhe veprimin e ndërmarrë lidhur me përpunimin e të dhënave personale, shkresën e vërtetimit të qasjes, shkresën e çdo qasjeje të paautorizuar dhe shkresën e refuzimit automatik të qasjes nga sistemi informatikë.

**7. Ndryshimi i cilësimeve standarde të sistemit CMS dhe garantimi i sigurisë së regjistrave të ueb-faqes deri në shkallën në të cilën aq sa është e mundur**

Sulmet më të zakonshme në ueb-faqet janë plotësisht të automatizuara. Ajo në çfarë shpresojnë shumë sulmues është fakti që përdoruesit t'i kenë lënë sistemet e tyre CMS





me cilësimet e fabrikës. Kur hakerët sulmojnë ndonjë ueb-faqe, ata duan të kenë qasje në bazën e të dhënave ose regjistrat e administrimit. Këto dy gjëra duhet të jenë në fokusin e kontrollorëve kur i sigurojnë ueb-faqet e tyre. Duhet mbajtur mend se të gjitha sulmet e hakerëve gjithnjë i synojnë këto dy fusha. Hakerët shpesh i skanojnë regjistrat me emra si "admin" ose "hyr". Nëse ekziston opsioni i tillë, këta regjistra duhet të rëmërohen. Nëse nuk mund të rëmërohen, atëherë duhet të ndryshohet leja për t'iu qasur atyre dhe datotekave të tjerë të ndjeshëm. Fshirja ose rregullimi i dosarëve dhe datotekave duhet të kufizohet, përkatësisht të pamundësohet pa lejen e kontrollorit.

#### 8. Krijimi i kopjes rezervë / kopjes së sigurt të ueb-faqes

Siç u përmend lidhur me krijimin e kopjeve rezervë të të dhënave, ekzistojnë arsye të ndryshme që mund të çojnë në humbjen e të dhënave të ueb-faqes. Për shembull, ueb-serveri mund të bjerë ose të infektohet me virus që do t'i shkatërrojë të dhënat, ndonjë punonjës mund t'i fshijë me qëllim ose pa qëllim të dhënat, të dhënat mund të shkatërrohen nga sulmi i hakerëve ose mund të ndodhë katastrofa natyrore (zjarri, tërmeti, përmytja, etj.). Për këto arsye ueb-faqet duhet të kenë kopje rezervë. Kopja e tillë duhet të ekzistojë për të gjithë ueb-faqen dhe datotekat e saj në vend të veçantë, siç rregullohet në nenin 22 të Rregullores dhe siç theksohet në kapitullin për krijimin e kopjeve rezervë të këtij udhërrëfyesi.

#### 9. Të njohurit e datotekave për konfigurimin e ueb-serverit

Punonjësit që kishin autorizime për të administruar ueb-faqen duhet t'i dinë datotekat e konfigurimit të ueb-serverit ku është vendosur ueb-faqja. Ato mund të gjenden në regjistrin kryesor të ueb-faqes dhe mundësojnë administrimin e rregullave të serverit. Ueb-serverë të ndryshëm përdorin lloj të ndryshëm të datotekave, për shembull, ueb-serverët Apache përdorin datoteka të llojit .htaccess, ndërsa serverët Nginx përdorin nginx.conf, serverët e Microsoft IIS përdorin datoteka të llojit web.config.

#### 10. Përdorimi i murit mbrojtës për ueb-aplikacionet

Në ueb-faqen duhet të përdoret muri mbrojtës i ueb-aplikacioneve (WAF). Ai duhet të vendoset midis serverit të ueb-faqes dhe lidhjes së të dhënave, ndërsa qëllimi i këtij muri mbrojtës është të lexojë çdo bit të të dhënave që kalojnë përmes tij për të mbrojtur ueb-faqen. Gjithashtu, muri mbrojtës mund të filtrojë lloje të tjera të komunikacionit të padëshiruar përmes internetit, për shembull, spamët dhe botot me qëllim të keq.

#### 11. Forcimi i sigurisë së rrjetit

Kontrollorët duhet të analizojnë sigurinë e rrjetit të tyre. Punonjësit me autorizime të administrimit të ueb-faqes mund të krijojnë pa qëllim shteg të pasigurt për në ueb-faqen. Për të parandaluar mundësimin e qasjes së tillë në ueb-serverin, rekomandohet që kontrollorët t'i ndër marrin hapat e mëposhtëm:

- cilësimet për hyrjen përmes kompjuterit që skadon pas një periudhe të caktuar të shkurtër të pasivitetit;
- cilësimet për sistemin për t'i njoftuar përdoruesit për ndryshimin e fjalëkalimit çdo tre muaj;
- sigurimi që të gjitha pajisjet e lidhura në rrjet skanohen për programe me qëllime të këqija çdoherë kur ato lidhen në rrjet.





### 6.1.8 Parandalimi, reagimi dhe kthimi i sistemit pas incidenteve (sigurimi i vazhdimësisë)

Në bazë të analizës së zbatuar të rreziqeve dhe rreziqet që janë përcaktuar dhe që mund të prishin vazhdimësinë e proceseve që nënkuptojnë përpunimin e të dhënave personale dhe probabilitetin që ato të ndodhin, kontrollorët duhet të hartojnë plane për menaxhimin e vazhdimësisë së sistemeve të tyre informatike. Këto plane duhet të përfshijnë aksione që ndërmerren për të parandaluar rreziqet e tilla, listë të personave të autorizuar që janë përgjegjës për parandalimin e çdo rreziku të mundshëm që ishte identifikuar si kërcënim për vazhdimësinë e përpunimit. Si pjesë e të njëjtit plan ose si plan i veçantë, kontrollorët duhet të përcaktojnë aksione që duhet ndërmarrë në rast se ndonjë rrezik materializohet, duke përfshirë edhe listën e personave të autorizuar që janë përgjegjës për kthimin e sistemit në gjendje normale, kategoritë e të dhënave personale që do të kthehen ose kategoritë e të dhënave personale që do të futen me dorë në sistem si pjesë e kthimit të tij në gjendjen fillestare për çdo rrezik që ishte identifikuar si kërcënim i mundshëm për vazhdimësinë e përpunimit me qëllim që sistemi të kthehet në gjendjen normale sa është e mundur më herët. Të gjithë punonjësit e kontrollorit duhet të jenë të njohur me planet e menaxhimit të vazhdimësisë së sistemit informatikë, si dhe rolin e tyre brenda atij plani për t'i shmangur anulimet në procedurat e reagimit dhe kthimit. Kontrollorët sigurojnë që personat e autorizuar, përpunuesit dhe nënpërpunuesit janë të vetëdijshëm për rastet kur duhet të alarmohet dhe të parashtrahet njoftimi për incidentet.

Parandalimi i incidenteve përfshin masa dhe kontrollime, të tilla siç janë përcaktuar në Rregulloren, të cilat bazohen në analizën e zbatuar të rreziqeve dhe theksohen në dokumentet interne të kontrollorit (për shembull, përdorimi i pajisjeve për furnizimin e pandërprerë me energji elektrike për të mbrojtur pajisjen që përdoret për përpunimin e të dhënave në rast të rënies së sistemit të furnizimit me energji elektrike, teknologjisë RAID (një sërë rezervash të disqeve të lira), testimi i rregullt i funksionimit të pajisjeve, edukimi i rregullt i punonjësve për mbrojtjen e të dhënave personale, etj.).

### 6.1.9 Kopjet rezervë dhe kthimi i të dhënave personale (sigurimi i vazhdimësisë)

Ekzistojnë arsye të ndryshme që mund të çojnë në humbjen e të dhënave në ndonjë organizatë, për shembull, prishja e diskut të kompjuterit, thyerja e telefonit ose tabletit inteligjent, infektimi i kompjuterit ose pajisjeve të lëvizshme me virus që i shkatërron të dhënat, fshirja e qëllimshme ose e paqëllimshme e të dhënave nga punonjësi, shkatërrimi i të dhënave nga sulmet e hakerëve, katastrofa natyrore (zjarri, tërmeti, përmytja), etj. Për këto arsye, është e nevojshme të ekzistojë kopja rezervë e të dhënave që i mundëson organizatës të funksionojë pa probleme dhe ta bëjë të aftë që të vazhdojë punën edhe në rrethana të tilla të parashikuara.

Në bazë të analizës së zbatuar të rreziqeve, krijimi cilësor i kopjeve rezervë të të dhënave imponon zbatimin e hapave të mëposhtëm:

#### 1. Identifikimi i të dhënave për të cilat bëhet kopja rezervë

Në varësi të veprimtarisë, çdo organizatë vendos se cilat të dhëna janë të rëndësishme për funksionimin e vazhdueshëm të saj dhe për cilat detyrimisht duhet të ekzistojë kopja rezervë. Në thelb, kopjet rezervë duhet të bëhen nga të gjitha të dhënat që nuk mund të jenë të thjeshta dhe lehtësisht të kthyeshme ose nuk mund të zëvendësohen në rast të humbjes.





## 2. Përcaktimi i mediumit për ruajtjen e kopjeve rezervë

Zgjedhja e mediumit për kopjet rezervë varet nga rëndësia e të dhënave për të cilat bëhet kopja rezervë, afatet e ruajtjes së kopjes rezervë, sa shpesh bëhet kopja rezervë, si dhe aftësitë e organizatës për të bërë kopje rezervë. Mediumet e ruajtjes së kopjeve rezervë mund të jenë CD/DVD, disku USB, disku i jashtëm, shiriti magnetik, sistemi i disqeve, kopja rezervë në re, etj.

## 3. Përcaktimi i lokacionit të kopjeve rezervë të të dhënave

Mediumet me kopjet rezervë të të dhënave duhet të ruhen në vend të sigurt (p.sh. të mbyllur në sirtar të papërshkueshëm nga zjarri) në të cilin kanë qasje vetëm personat e autorizuar brenda organizatës. Në kushtet ideale, mediumet me kopjet rezervë duhet të ruhen në vend që është i sigurt dhe mjaft larg nga vendi origjinal i të dhënave që do të mundësojë kthimin e sigurt të të dhënave dhe funksionimin normal në rast të katastrofës natyrore ose dëmit tjetër të vëllimit të madh.

## 4. Përcaktimi i afatit dhe mënyrës për ruajtjen e kopjeve rezervë

Afati i ruajtjes dhe mënyra e krijimit të kopjeve rezervë (nëse kopja rezervë bëhet në të gjitha të dhënat ose vetëm në ato që janë ndryshuar, respektivisht në të dhënat e reja) përcaktohet në varësi të përkufizimit të shpeshtësisë së ndryshimit të të dhënave dhe vëllimit të të dhënave që duhet të ruhen. Kopjet e tilla rezervë mund të bëhen menjëherë pas paraqitjes së të dhënave, periodikisht gjatë një dite, një herë në ditë, një herë në javë, dy herë në muaj, një herë në muaj, një herë në gjashtë muaj ose një herë në vit. Në praktikë, zakonisht bëhen kopje rezervë periodike për datotekat që ishin krijuar nga programi tekstual ose tabelar, për bazat e të dhënave të përdorura nga programet kompjuterike, e-posta, etj., ndërsa kopja rezervë e programeve kompjuterike dhe sistemeve operative bëhet përpara përditësimeve të mëdha ose instalimit të versioneve më të reja. Për shembull, në fund të ditës së punës bëhet kopja rezervë e datotekave në të cilat është bërë ndryshimi, kopja rezervë në javë bëhet në datotekat e specifikuar konkretë, e-posta dhe baza e të dhënave që nuk ndryshojnë shpesh, dhe kopja rezervë në muaj, gjysmëvjetore ose vjetore bëhen për të gjithë kompjuterin.

## 5. Testimi i kopjeve rezervë të të dhënave

Për të siguruar që të dhënat mund të kthehen me sukses dhe të përdoren nga kopja rezervë, nga kopja e tillë duhet të bëhet kopja e re rezervë dhe ajo duhet të testohet.

Testimi i kopjes rezervë rekomandohet në rastet e mëposhtme:

- pas krijimit të kopjes së parë rezervë, duhet të sigurohet që ajo është bërë me korrektësi dhe që programet, bazat e të dhënave dhe/ose datotekat mund të kthehen në mënyrë të sigurt;
- pas blerjes së kompjuterit të ri, duhet të sigurohet që të gjitha datotekat, bazat e të dhënave dhe programet e nevojshme mund të përdoren në kompjuterin e ri;
- pas përditësimit të madh të sistemit operativ ekzistues ose pas përditësimit me versionin më të ri të sistemit operativ, duhet të sigurohet që ndryshimet në sistem nuk ndikojnë në funksionimin përkatës të programit dhe përdorimin e pandërprerë të datotekave dhe bazave të të dhënave;
- pas përditësimit të programit ose instalimit të programit që krijon lloje tekstuale, tabelare ose lloje të tjera të datotekave në të cilat ruhen të dhënat, duhet të sigurohet që datotekat mund në mënyrë përkatëse të hapen dhe të përdoren;
- kontrollohet periodikisht që mediumet në të cilat ruhen kopjet rezervë të të dhënave nuk janë dëmtuar.





Nga madhësia e organizatës, vëllimi i të dhënave që u përpunuan dhe kompleksiteti i proceseve të punës varet edhe mënyra në të cilën bëhen kopjet rezervë të të dhënave. Për shembull, salloni i floktarisë që përdor një kompjuter për të përpunuar të dhënat e ruajtura në datotekat tekstuale ose tabelare, mund të përdor program që është i integruar në sistemin operativ ose ndonjë nga programet e kompresimit për të krijuar datotekë që shërben si kopje rezervë, ndërsa për ta ruajtur atë mund të përdor disk portativ ose pajisje USB me kapacitet përkatës. Natyrisht, nuk ka dyshim se duhet të zbatohen të gjitha masat për mbrojtjen e të dhënave personale të përcaktuara për softuerin e tillë ose mediumin për ruajtjen e të dhënave. Nga ana tjetër, shitorja për pjesët rezervë të automjeteve që përdor programe të ndryshme për ruajtjen e të dhënave në bazën e të dhënave dhe që përpunon vëllim të madh të të dhënave, ndoshta mund të blejë program të dedikuar për krijimin automatik të kopjeve rezervë, si dhe medium për ruajtjen e të dhënave me kapacitet më të madh se disku portativ ose disku për ruajtjen e të dhënave.

Nëse ndonjë organizatë vendos që krijimin e kopjeve rezervë t'ia besojë bashkëpunëtorit të jashtëm që ofron shërbime kompjuterike dhe ruajtjen e të dhënave në re, duhet të kontrollohet nëse ofruesi i këtyre shërbimeve ofron dhe garanton nivel të lartë të sigurisë për të dhënat që ruhen në atë mënyrë, përkatësisht nëse të dhënat ruhen në formë të kriptuar, nëse ofruesi i shërbimeve zbaton nivel të lartë të mbrojtjes nga qasja e paautorizuar deri në të dhënat, nëse ofron lidhje të sigurt të internetit (VPN) ndërmjet përdoruesve dhe resë, dhe nëse i zbaton të gjitha masat e tjera teknike dhe organizative që sigurojnë nivel të barabartë të mbrojtjes së të dhënave personale.

#### 6.1.10 Mënyra e arkivimit dhe ruajtjes së të dhënave

Ekzistojnë të dhëna të caktuara personale që nuk janë të nevojshme për përpunimin e drejtpërdrejtë dhe të përditshëm dhe të cilat, për shkak të rregullave të përcaktuara me ligj që përfshin përpunimin në fjalë, duhet të arkivohen ose ruhen në periudhë të caktuar ligjore. Për shembull, kompania që ofron shërbime të telefonisë fikse dhe lidh kontrata dyvjeçare me përdoruesin. Kontrata dhe të dhënat personale duhet të përpunohen dhe ruhen deri në përmbushjen e qëllimit, përkatësisht deri në skadimin e kontratës (plus periudha e parashkrimit të kërkesave), ndërsa faturat ruhen si dokumente të kontabilitetit në përputhje me rregullat ligjore. Shembull tjetër janë të dhënat personale të punonjësve të përpunuara nga Departamenti i Resurseve Njerëzore dhe Departamenti i Financave. Pasi personi tashmë nuk është punësuar në organizatë, këto departamente duhet të arkivojnë të dhëna të caktuara të përcaktuara me ligj dhe t'i ruajnë për një periudhë të caktuar të përkufizuar në atë ligj (Departamenti i Resurseve Njerëzore e zbaton Ligjin për marrëdhënie pune, ndërsa Departamenti i Financave e zbaton Ligjin për rroga).

Të dhënat e tilla personale duhet të arkivohen në mënyrë të sigurt, veçanërisht kur të dhënat e arkivuara janë me natyrë të ndjeshme (p.sh. kategoritë e veçanta të të dhënave personale ose të dhënat personale të fëmijëve) ose ato mund të ndikojnë seriozisht në të drejtat e subjekteve të të dhënave personale në rast se kompromitohen.

Duke pasur parasysh se të dhënat personale që duhet të arkivohen mund të ruhen në formë digjitale dhe/ose në letër, për të siguruar arkivimin dhe ruajtjen përkatëse të të dhënave të tilla, kontrollori vendos procedura për menaxhimin e materialit arkivor për të dhënat e tilla, si dhe ku ruhen, si dhe në çfarë kushtesh mund t'u qasesh atyre.





Kontrollori duhet të miratojë dokument përkatës të titulluar "lista (pasqyra) e afateve për ruajtjen e të dhënave personale", e cila përmban informacione për momentin kur fillon perioda / afati për ruajtjen, arsyet e ruajtjes së të dhënave personale, bazën juridike për ruajtjen e të dhënave personale dhe pronarin e të dhënave të tilla. Gjithashtu, kontrollori duhet të kryejë kontrollim vjetor dhe harmonizim të këtij dokumenti me ndryshimet që u bënë në funksionimin e tij dhe me kërkesat ligjore për ruajtjen e të dhënave personale.

#### 6.1.11 Kriptimi i të dhënave personale

Kriptimi i përpunimit të të dhënave personale duhet të merret parasysh nga aspekti i kriptimit të qasjes në të dhënat personale, transmetimit të të dhënave personale përmes rrjeteve të komunikimit elektronik dhe ruajtjes së të dhënave personale në formën e kriptuar.

Për secilin nga aspektet e mësipërme, kontrollorët duhet të përdorin algoritme të kriptimit të njohura dhe të sigurta në mënyrë përkatëse të cilat zbatohen për aspektin konkret dhe bazohen në analizën e zbatuar të rreziqeve.

Nga aspekti i kriptimit të qasjes në sistemet operative të përpunimit të të dhënave personale, ekzistojnë programe komerciale dhe sisteme të menaxhimit që zbatojnë algoritme përkatëse të kriptimit për të ruajtur emrat e përdoruesve dhe fjalëkalimet dhe mund të përdoren për qasjen e autorizuar. Kontrollorët duhet të ndërmarrin masat përkatëse për të zbatuar algoritme të njohura dhe të sigurta të kriptimit (p.sh., bcrypt, scrypt ose PBKDF2) për qëllimet e ruajtjes së fjalëkalimeve. Së bashku me kompaninë që zhvillon softuerin e tyre, kontrollorët duhet të kontrollojnë nëse janë zbatuar algoritmet përkatëse për të mbajtur mend emrat e përdoruesve dhe fjalëkalimet e autorizuar në mënyrë të sigurt. Në këtë kuptim dhe në bazë të analizës së zbatuar të rreziqeve, kontrollorët duhet të mendojnë për atë se edhe disqet e deponimit që janë pjesë e pajisjeve të lëvizshme (disqeve) dhe mediumet e transmetimit (disqe të jashtëm, pajisje USB, CD ROM, DVD, kartela memorie, kartela SIM) duhet të kenë masa të forta të kriptimit në rast të humbjes, me qëllim që të dhënat që ruhen në to të mos lexohen pa qasjen e autorizuar. Nëse sistemi operativ i pajisjes së lëvizshme ofron kriptim të disqeve, duhet të përdoret opsioni i tillë, dhe në të kundërtën, kontrollorët duhet të përdorin softuer të besueshëm të dizajnuar për përdorimin e disqeve dhe mediumeve të transmetimit për ruajtjen e të dhënave që i zbatojnë rregullat për krijimin e fjalëkalimeve të forta. Aplikacionet e tilla duhet të përdorin algoritme të kriptimit tashmë të dëshmuara, për shembull, AES, Serpent, Twofish, Camellia, Kuznyechik ose kombinime kaskade të tyre për siguri shtesë me hash-funksione kriptografike të dëshmuara, për shembull, SHA-256, SHA-512, RIPEMD-160, etj.

Një aspekt tjetër është kriptimi i të dhënave personale të transmetuara përmes rrjeteve të komunikimit elektronik. Në bazë të analizës së zbatuar të rreziqeve, kontrollorët miratojnë vendim nëse edhe komunikimi lokal i rrjetit duhet të kriptohej, të paktën në rastin e shkëmbimit online të të dhënave midis ueb-faqes dhe ueb-serverit. Si standard minimal, komunikimi i tillë duhet të kriptohej me protokoll kriptografik të dizajnuar për të mundësuar sigurinë e komunikimeve që ndodhin përmes rrjetit kompjuterik (p.sh., TLS1.3). Përveç kësaj, nëse ka nevojë për qasje nga distanca nëpërmjet internetit në rrjetin informatikë intern ose ka nevojë për të vendosur lidhje nëpërmjet internetit midis dy organizatave në lokacione të veçanta, lidhja e tillë duhet të vendoset nëpërmjet lidhjes VPN duke zbatuar protokolle dhe algoritme të njohura dhe të sigurta të kriptimit (p.sh., L2TP dhe IPSec, SSTP, etj.) me





vërtetimin e detyrueshëm të personave të autorizuar (p.sh., kartela inteligjente, pajisja e gjenerimit të fjalëkalimit të njehershëm, etj.

Aspekti i tretë është ruajtja e të dhënave personale në formë të kriptuar. Në bazë të analizës së zbatuar të rreziqeve, kontrollori duhet të përcaktojë se cilat të dhëna personale duhet të ruhen në formë të kriptuar me qëllim që të dhënat e tilla të bëhen të padobishme në rast të qasjes së paautorizuar në vendin ku ruhen pa njohjen e algoritmit ose çelësin e dekriptimit. Algoritmet e kriptimit duhet të instalohen në kodin e programeve të punës dhe në varësi të analizës së zbatuar të rreziqeve, duhet të përdoren algoritme përkatëse të kriptimit (p.sh., AES ose AES-CBC për kriptimin simetrik, RSA-OAEP v2.1 për kriptimin asimetrik, etj.) dhe për dekriptimin (p.sh., DES, Triple DES, TRIPLE\_DES\_3KEY, RC2, RC4, 128-bit RC4, DESX, 128-bit AES, 192-bit AES, dhe 256-bit AES, etj.). Si standard minimal, rekomandohet në formë të kriptuar të ruhen kategoritë e veçanta të të dhënave personale, të dhënat personale të fëmijëve ose të dhënat personale që mund të kenë ndikim serioz në të drejtat e subjekteve të të dhënave personale në rast se ato kompromitohen.

Kontrollori mund t'i përdor shërbimet e përpunuesit për të ruajtur të dhënat jashtë hapësirave të tij dhe/ose të përdor programe softuerike të përpunimit që mund të vendosen fizikisht, të hostohen dhe të administrohen jashtë hapësirave të tij. Në rast të tillë, kontrollori duhet t'i rregullojë të drejtat dhe detyrimet e ndërsjella me përpunuesin në formën e kontratës me shkrim, e cila duhet të përfshijë edhe dispozita për masat e sigurisë së të dhënave personale në përputhje me rregullat për mbrojtjen e të dhënave personale. Përpara lidhjes së kontratës, kontrollori duhet të kontrollojë nëse përpunuesi zbaton masat teknike dhe organizative përkatëse për mbrojtjen e të dhënave personale, dhe sipas këtij kapitulli, nëse i përmbush kërkesat për kriptim nga të gjitha aspektet e theksuara më sipër. Në bazë të analizës së zbatuar të rreziqeve, kontrollori duhet të përcaktojë nëse të gjitha të dhënat personale duhet të kriptohen përpara se të ruhen në sistemin informatikë të përpunuesit.

Kontrollori miraton procedura interne që e përcaktojnë mënyrën e menaxhimit të çelësive dhe certifikatave sekrete, duke e marrë parasysh menaxhimin e rreziqeve që lidhen me fjalëkalimet e harruara.

#### **6.1.12 Shkëmbimi i të dhënave përmes postës elektronike**

Posta elektronike (e-posta), dhe veçanërisht posta elektronike përmes serviseve publike (Gmail, Hotmail, Yahoo Mail...) është mënyrë shumë e pasigurt e komunikimit dhe shkëmbimit të të dhënave. Megjithëse komunikimi përmes e-postës mund të kriptohet me protokollin SSL/TLS, nëse serveri i e-postës i dërguesit ose pranuesit nuk mbështet protokoll të tillë, përmbajtja e e-postës do të transmetohet si e pakriptuar. Gjithashtu, porositë elektronike ruhen në serverin e e-postës në formë të pakriptuar.

Si masë e sigurisë, e gjithë përmbajtja e e-porosive mund të kriptohet me vegël të besueshme të kriptimit (Public Key Infrastructure) të dedikuar për e-postë (p.sh., PGP ose S/MIME). Duke përdorur këtë metodë, pranuesi duhet të krijojë çelës publik për kriptim dhe çelës publik për dekriptim. Dërguesi e kripton e-porosinë me çelësin publik të pranuesit, ndërsa më pas pranuesi e dekripton përmbajtjen me çelës tjetër privat.

Më poshtë janë shembujt e masave të tjera që duhet të merren parasysh kur dërgoni e-postë:





- teksti i e-porosisë mos të përmbajë të dhëna personale që nuk u referohen të dhënave të punës së kontaktit, dhe veçanërisht mos të përmbajë të dhëna personale të palëve të treta (persona që nuk janë dërguesi ose pranuesi);
- të dhënat personale të cilat ruhen në formë digjitale të kriptohen me program softuerik për kompresimin e të dhënave që ka aftësinë për të kriptuar përmbajtjen e arkivit me algoritme të besueshme të kriptimit (p.sh., AES-256) dhe të mbrohen me fjalëkalim të fortë, pas së cilës datoteka e mbrojtur dërgohet si bashkëngjitje në e-porositë;
- fjalëkalimi i dekriptimit duhet t'i dërgohet pranuesit përmes kanalit tjetër të komunikimit (p.sh., përmes telefonit, SMS, etj.) dhe jo përmes e-postës.

### 6.1.13 Siguria fizike

Kur ndonjë organizatë vendos masa të sigurisë, ajo duhet të mendojë edhe për vendosjen e masave fizike përkatëse për mbrojtje nga qasja e paautorizuar në hapësirat e saj dhe në pajisjen që e përdor.

Gjatë vendosjes së masave të sigurisë fizike, duhet të merret parasysh kjo si në vijim:

- sigurimi i objektit nga qasja e paautorizuar jashtë orëve të punës së organizatës (p.sh., duke instaluar alarme për vjedhje dhe sistem të video-mbikqyrjes, nëse vlerësimi i rrezikut tregon se ky është i nevojshëm dhe i justifikuar), dhe kontrollimi periodik i nivelit të funksionalitetit;
- kufizimi i qasjes në pajisjen në të cilën ruhen të dhënat personale (serverët e kompjuterit, sistemet e diskut, disqet eksterne, të dhënat në formë letre, etj.) duke vendosur pajisjen e tillë në mobiljet përkatëse të zyrës (p.sh. raftet për serverët për të dhënat digjitale, dollapët metalikë për të dhënat në formë letre) dhe dhomat e zyrës (p.sh. dhoma e serverëve) ose hapësirat / zyrat që mbrohen në mënyrë adekuate nga qasja e paautorizuar (p.sh., duke përdorur çelësa ose kartela inteligjente që u jepen vetëm personave të autorizuar);
- kufizimi i qasjes në mobiljet e zyrës (p.sh., raftet e serverëve ose dollapët metalikë) dhe dhomat e zyrës (respektivisht dhoma e serverit ose arkivi) ku ruhen të dhënat personale dhe të dhënat e tjera konfidenciale (p.sh., hapësirat që çojnë në dhomën e serverëve ku janë të vendosur kompjuterët / serverët, në të cilat ruhen të dhënat, hapësirat / dhomat ose dollapët ku ruhen të dhënat në formë letre);
- mbajtja e evidencës për qasjen në hapësirat ku janë të vendosur serverët që përmbajnë të dhëna personale në formë digjitale ose hapësirat ku ruhen të dhënat në formë letre dhe, kur është e përshtatshme, mbajtja e evidencës së përpjekjeve për qasjen e paautorizuar në këto fusha;
- meqë serverët kompjuterikë, disqet dhe pajisja tjetër digjitale për ruajtjen e vëllimit të madh të të dhënave janë lëndë e rreziqeve më serioze, nevojiten më shumë masa të sigurisë në hapësirat dhe dhomat e serverëve ku vendoset pajisja e tillë. Duke i marrë parasysh teknologjitë më moderne, shpenzimi i zbatimit dhe natyra, vëllimi, konteksti dhe qëllimi i përpunimit, si dhe rreziqet e probabilitetit dhe seriozitetit të ndryshëm ndaj të drejtave dhe lirive të personave fizikë që rezultojnë nga përpunimi, kur përcaktojnë mjetet e përpunimit dhe gjatë përpunimit të të dhënave personale, kontrollorët zbatojnë masat teknike përkatëse për të mbrojtur pajisjet dhe hapësirat në të cilat është vendosur pajisja nga fatkeqësitë natyrore, të tilla si zjarret, tymi, uji,





pluhuri, dridhjet, substancat kimike, ndërprerjet e furnizimit me energji elektrike dhe rrezatimi elektromagnetik (p.sh., dhoma e serverëve duhet të ndërtohet me mbrojtje kundër zjarrit, ndërsa kur kjo nuk është e zbatueshme, atëherë ajo duhet të mbrohet nga sistemi përkatës kundër zjarrit që është përkatës për pajisjen elektronike; të jetë i ndërtuar nga materiali i papërshkueshëm nga uji, ndërsa kur kjo nuk është e zbatueshme, atëherë kjo duhet të ketë dysheme të ngritur antistatik dhe sistem për rrjedhje; të jetë e pajisur me sistem të ftohjes për të cilin ekziston sistemi rezervë, respektivisht klimatizimi; të ketë furnizim të pandërprerë me energji elektrike për të siguruar vazhdimësinë ose të paktën mbylljen e sigurt të të gjitha pajisjeve derisa të kthehet furnizimi me energji elektrike);

- zbatimi i masave teknike përkatëse si ato të dhëna më sipër, por të përshtatura për të mbrojtur të dhënat e ruajtura në formë letre (p.sh., hapësirat duhet të jenë të ndërtuara nga materiali i papërshkueshëm nga zjarri, ndërsa kur kjo nuk është e zbatueshme, atëherë ato duhet të pajisen me sistem kundër zjarrit që është përkatës për mbrojtjen e letrës; të ndërtohen me material të papërshkueshëm nga uji, ndërsa kur kjo nuk është e zbatueshme, atëherë duhet të kenë ngritur dysheme dhe sistem të rrjedhjes; të kenë sistem të klimatizimit për të mbajtur nivel përkatës të lagështisë dhe temperaturë në hapësirat, etj.);
- vendosja e pajisjes tjetër të rrjetit të komunikimit (p.sh., ruteri i internetit, ndërprerësit e rrjetit, etj.) në mobiljet përkatëse të zyrës (p.sh., raftet e serverëve) dhe/ose në hapësirat që janë të mbrojtura në mënyrë adekuate nga qasja e paautorizuar (p.sh., me çelës ose kartelë inteligjente);
- sigurimi që të gjitha pajisjet thelbësore të sistemit informatikë (serverët, kompjuterët, pajisjet e rrjetit lokal, pajisjet e rrjetit, të tillë si printerët, etj.) ka furnizim të pandërprerë me energji elektrike për të siguruar vazhdimësinë ose të paktën mbylljen e sigurt të të gjitha pajisjeve derisa të kthehet furnizimi me energji elektrike);
- pajisja e zyrës (kompjuterët, printerët, makinat e fotokopjimit, etj.) të përdorura për punë ndërvepruese me klientët e shërbimeve të punës për t'u ndarë fizikisht nga përdoruesit ose të paktën për të vështirësuar qasjen e klientëve në pajisjen e tillë dhe në të dhënat (p.sh., pengesa fizike midis përdoruesve dhe hapësirës së punës), përkatësisht të ekzistojë sporteli që e pengon përdoruesin të ketë qasje në pajisjet, printerët, makinat e fotokopjimit në të cilën ruhen të dhënat në formë letre me atë që ato do të jetë mjaft larg për përdoruesin që mos të ketë inspektim në të dhënat, monitori i kompjuterit është i kthyer me anën e pasme drejt përdoruesit, etj.);
- zbatimi i rregullit "byroja e pastër" në mënyrën që siguron që të gjitha dokumentet e rëndësishme, letrat konfidenciale, dosarët, librat etj., të hiqen nga byroja dhe të mbyllën kur nuk janë në përdorim ose kur punonjësi largohet nga stacioni i tij i punës. Kjo është një nga strategjitë kryesore të aplikuara për të reduktuar rrezikun e shkeljes së sigurisë së të dhënave personale. Përveç kësaj, në hapësirën e punës nuk duhet të ketë fletë vetëngjithëse me shënime, dokumente me informacione, të tilla si letërnjoftimi i përdoruesit, fjalëkalimet ose numrat e llogarisë bankare dhe duhet të jetë e liruar nga të gjitha dokumentet jothelbësore.





Kontrollorët mund të përdorin shërbimet e përpunuesit për të ruajtur të dhënat personale jashtë hapësirave të tyre dhe/ose të përdorin programe të përpunimit që mund të gjenden fizikisht, të hostuar dhe të administruar jashtë hapësirave të tyre (p.sh. ueb-serveri i organizatës mund të hostohet jashtë hapësirave të kontrollorit).

Në rast të tillë, kontrollori duhet t'i rregullojë të drejtat dhe detyrimet e ndërsjella me përpunuesin në formën e kontratës me shkrim që duhet të përfshijë dispozita për masat e sigurisë së të dhënave personale në përputhje me rregullat për mbrojtjen e të dhënave personale.

Përpara lidhjes së kontratës, kontrollori duhet të kontrollojë nëse përpunuesi zbaton masat teknike dhe organizative përkatëse për mbrojtjen e të dhënave personale.

#### **6.1.14 Kontrollimi i sistemit informatikë dhe infrastrukturës**

Siç u tha më parë, të gjitha masat teknike dhe organizative të përcaktuara në ZMDHP-në dhe Rregulloren, si dhe në dokumentet interne të kontrollorit që u referohen masave teknike dhe organizative, nuk do të kenë kurrfarë efekti nëse të gjithë punonjësit e kontrollorit nuk i zbatojnë rregullisht. Si rrjedhojë, dokumentacioni për masat teknike dhe organizative të kontrollorit duhet të përfshijë edhe procedurën për autorizimin e oficerit për mbrojtjen e të dhënave personale në mënyrë që ai/ajo të mund të kryejë kontrollime periodike për të ndjekur harmonizimin e kontrollorit me rregullat për mbrojtjen e të dhënave personale dhe dokumentacionin e miratuar për masat teknike dhe organizative. Sistemi informatikë dhe infrastruktura e kontrollorit duhet të jetë lëndë e kontrollimit intern për të kontrolluar nëse zbatohen procedurat dhe udhëzimet e dhëna në rregullat dhe politikat për sigurinë e të dhënave personale dhe nëse ato janë në përputhje me rregullat për mbrojtjen e të dhënave personale.

#### **6.1.15 Menaxhimi i përpunuesve dhe angazhimi i përpunuesve**

Nëse kontrollori vendos të përdor ndonjë përpunim të të dhënave personale të ofruara nga subjekti tjetër i punës (përpunues), atëherë ai është i detyruar të zbatojë procedurë për zgjedhjen e përpunuesit përkatës që duhet të parashikojë këtë si në vijim:

- analizën e përpunuesve potencialë përta u përket masave të tyre teknike dhe organizative që garantojnë që përpunimi të kryhet në përputhje me kushtet e përcaktuara në rregullat për mbrojtjen e të dhënave personale dhe nivelin e mbrojtjes që është përkatës me të dhënat personale të përpunuara nga kontrollori, dhe garantojnë mbrojtjen e të drejtave të subjekteve të të dhënave personale;
- analizën e rreziqeve në punën e kontrollorit që mund të dalin nga përpunimi i të dhënave personale nga përpunuesit.

Në mënyrë plotësuese, në vendosjen e procedurës për përzgjedhjen e përpunuesve, kontrollorët janë të detyruar të vendosin procese për menaxhimin e përdorimit të shërbimeve të ofruara nga përpunuesit dhe në lidhje me menaxhimin e përpunimit dhe të sigurojnë përmbushjen e detyrimeve dhe përgjegjësi kontraktuese nga përpunuesit e angazhuar.

Si rrjedhojë, kontrollorët mund t'i delegojnë detyrat në lidhje me përpunimin e të dhënave personale në emër të tyre vetëm për përpunuesit që ofrojnë garanci të mjaftueshme, veçanërisht në lidhje me njohuritë, sigurinë dhe resurset e nevojshme në fushën e mbrojtjes së të dhënave personale.





Edhe kur përpunuesit i kanë deleguar detyrat që janë pjesë e punës së kryer nga kontrollori dhe kanë të bëjnë me përpunimin e të dhënave personale, kontrollorët janë të detyruar të sigurojnë kontrollim mbi përpunimin e tillë lidhur me sigurinë e të dhënave personale, ku të dhënat përpunohen duke zbatuar masat përkatëse të sigurisë.

Të drejtat dhe detyrimet e ndërsjella të kontrollorit dhe përpunuesit duhet të rregullohen me kontratë me shkrim, ndërsa përpara nënshkrimit të kontratës së tillë, kontrollori është i detyruar të kërkojë nga ofruesi i shërbimit (përpunuesi) inspektim në politikën e tij të sigurisë që i referohet sistemit informatikë dhe infrastrukturës së përdorur për përpunimin e të dhënave personale në emër të kontrollorit, ndërkohë që politika e tillë e sigurisë duhet të përmbajë informacione që garantojnë sigurinë e të dhënave personale, përkatësisht:

- nëse dhe si kriptohen të dhënat personale sipas ndjeshmërisë së tyre;
- a ekzistojnë procedura që garantojnë se asnjë person nuk do të ketë qasje të paautorizuar në të dhënat;
- nëse dhe si kriptohen të dhënat personale që transmetohen;
- garancitë në lidhje me gjurmueshmërinë (logot, gjurmët e informacioneve, etj.)
- menaxhimi i autorizimeve për qasje;
- vërtetimi;
- masat e tjera të sigurisë për përpunimin e të dhënave personale që janë të përshtatshme për përpunimin e të dhënave personale në fjalë.

Pastaj, kontrollori dhe përpunuesi lidhin kontratë që përmban dispozita lidhur me faktin si në vijim:

- lënda, kohëzgjatja dhe qëllimi i përpunimit të të dhënave personale;
- detyrimet e përpunuesit për të zbatuar masat teknike dhe organizative për të garantuar sigurinë e përpunimit;
- detyrimet lidhur me konfidencialitetin e të dhënave personale të dhëna;
- standardet minimale për vërtetimin e personave të autorizuar;
- kushtet për kthimin e të dhënave dhe/ose shkatërrimin e të dhënave pas skadimit ose ndërprerjes së kontratës;
- rregullat për menaxhimin e incidenteve dhe parashtrimin e njoftimit të kontrollorit në rast të shkeljes së sigurisë së të dhënave personale;
- detyrimi i përpunuesit për të ndërmarrë veprim sipas udhëzimeve të dhëna nga kontrollori;
- detyrimet dhe përgjegjësitë e tjera në përputhje me rregullat për mbrojtjen e të dhënave personale dhe dokumentacionin e miratuar për masat teknike dhe organizative.

## 6.2 Niveli i lartë i masave teknike

Përveç nivelit standard të masave teknike, në bazë të analizës së zbatuar të rreziqeve, kontrollorët zbatojnë edhe masa shtesë të sigurisë me qëllim që të demonstronjë harmonizimin shtesë me rregullat dhe praktikatat e mira për mbrojtjen e të dhënave personale.

Niveli i lartë i masave teknike përcaktohet në nenin 38 të Rregullores dhe u referohet masave shtesë që lidhen me menaxhimin e fjalëkalimeve. Pra, masa e parë e nivelit të lartë i referohet përdorimit të veglave të menaxhimit të fjalëkalimeve për të siguruar që fjalëkalimet e ndryshme për shërbime ose programe të ndryshme softuerike ruhen në mënyrë përkatëse





dhe për këtë qëllim duhet të përdor fjalëkalim kryesor për të pasur qasje në të gjitha fjalëkalimet të cilat duhet të jenë me kompleksitet të shtuar, respektivisht duhet të jetë kombinim prej të paktën 12 karaktereve alfanumerike (shkronja të mëdha dhe të vogla, simbole, numra dhe shenja speciale të pikësimit) dhe duhet të ndryshohet në interval të rregullt që nuk është më i gjatë se 30 ditë. Një masë tjetër e nivelit të lartë që bazohet në analizën e zbatuar të rreziqeve që u referohet rasteve kur persona të caktuar të autorizuar kanë nivel më të lartë të privilegjeve (p.sh., administratori i sistemit informatikë ose personat që krijojnë dhe përdorin fjalëkalim kryesor), me ç'rast kontrollorët mund të disperzojnë rrezikun duke menaxhuar fjalëkalimet me faktorët shtesë tek më shumë persona të autorizuar me nivel më të ulët të privilegjeve në përputhje me rregullin n-2, (p.sh. informacioni për fjalëkalimin ndahet me dy ose më tepër persona për hyrje të përbashkët, ndërsa secili prej tyre di vetëm një pjesë të fjalëkalimit, ose një person i autorizuar e di fjalëkalimin, ndërsa personi tjetër e posedon dhe e përdor kartelën inteligjente).

Neni 39 i Rregullores rregullon edhe një masë teknike të nivelit të lartë që ka të bëjë me certifikimin e mbrojtjes së të dhënave personale. Në mënyrë plotësuese me kontrollimin e brendshëm, kontrollorët mund - në bazë vullnetare - të vlerësojnë edhe proceset dhe dokumentet interne për mbrojtjen e të dhënave personale me qëllim të certifikimit të përpunimit të tyre të të dhënave personale me qëllim që të demonstrojnë harmonizim me rregullat për mbrojtjen e të dhënave personale. Procesi i certifikimit kryhet nga AMDHP-ja ose trupi tjetër i certifikimit në përputhje me rregullat për mbrojtjen e të dhënave personale.

Në nenin 40 të Rregullores përcaktohen masat që i referohen menaxhimit të medimeve të transmetimit. Sipas dispozitës së këtij neni, si masë teknike e nivelit të lartë, kontrollorët janë të detyruar të vendosin sistem për evidentimin e medimeve të transmetimit që i pranojnë me qëllim të mundësohet identifikimi i drejtpërdrejtë ose i tërthortë i medimeve të tilla, datën dhe vendin e pranimit, dërguesin, numrin e mediumit të pranuar, llojin e dokumenteve të regjistruara në medium, mënyrën se si janë dërguar mediumet, emrin / mbiemrin e personit të autorizuar për pranimin e medimeve të tilla. I njëjti sistem mund të zbatohet edhe për të mbajtur evidencën e medimeve që i dërgon kontrollori.

Masa teknike e nivelit të lartë e dhënë në nenin 41 të Rregullores nënkupton testimin e detyrueshëm të sistemit informatikë përpara zbatimit të tij dhe pas ndryshimeve të bëra në sistemin informatikë për të kontrolluar nëse sistemi garanton sigurinë e të dhënave personale në përputhje me rregullat për mbrojtjen e të dhënave personale. Testimi i sistemit informatikë nuk guxon të kryhet duke përpunuar të dhënat personale reale, por për këtë qëllim përdoren të dhënat personale imagjinare.

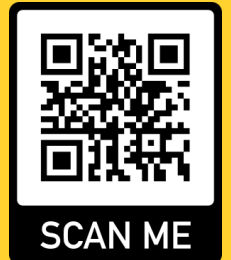
Neni 42 i Rregullores përcakton se kontrollorët mund të zbatojnë edhe masa të tjera teknike për të siguruar fshehtësinë dhe mbrojtjen e përpunimit të të dhënave personale përmes zbatimit të procedurave të certifikimit në përputhje me rregullat që rregullojnë përdorimin e dokumenteve elektronike, identifikimin elektronik dhe shërbimet konfidenciale.






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.**



SCAN ME

 +389 2 3230 635

 info@privacy.mk

 bul "Goce Dellçev" nr. 18  
Shkupi

 [www.azlp.mk](http://www.azlp.mk)



Ky projekt financohet nga Bashkimi Evropian

