UDHËZUES PËR OFICERË PËR MBROJTJE TË TË DHËNAVE PERSONALE NË INSTITUCIONE PUBLIKE

METAMORPHOSIS
Fondacion për internet dhe shoqëri

KONEKT

UDHËZUES PËR OFICERË PËR MBROJTJE TË TË DHËNAVE PERSONALE NË INSTITUCIONE PUBLIKE

METAMORPHOSIS
Fondacion për internet dhe shoqëri

KONEKT

Botues:
Fondacioni për Internet dhe Shoqëri - Metamorfozis

Autor:
Infigo IS

Redaktore:
Vesna Radinovska

Përktheu:
Bestel Sh.P.K.

Dizajni:
Evropa 92

Lektura:
Bestel Sh.P.K.

Shtypi:
Evropa 92 - Koçan

Tirazhi:
25 kopje

Tetor, 2023

METAMORPHOSIS
Fondacion për internet dhe shoqëri

KONEKT

PËRMBAJTJA

1. LISTA E SHKURTESAVE

AMDHP – Agjencia për Mbrojtjen e të Dhënave Personale

LMDHP – Ligji për mbrojtjen e të dhënave personale

OMDHP – Oficeri për mbrojtjen e të dhënave personale

GDPR – Rregullativa e përgjithshme për mbrojtjen e të dhënave personale (General Data Protection Regulation)

MSHIA – Ministria e Shoqërisë Informatike dhe Administratës

IA – Inteligjenca artificiale

EDPS – Mbikëqyrësi evropian për mbrojtjen e të dhënave personale (European Data Protection Supervisor)

VNDNJ – Vlerësimi i ndikimit mbi të drejtat e njeriut

2. HYRJE

Mbrojtja e të dhënave personale nuk është risi në sistemin juridik të Republikës së Maqedonisë së Veriut e as në shtetet e Bashkimit Evropian. Megjithatë, kjo e drejtë e njeriut e ka fituar popullaritetin sidomos pas miratimit të Rregullativës së përgjithshme për mbrojtjen e të dhënave personale (General Data Protection Regulation 2016/6792[1] - GDPR) në vitin 2016, e cila që për befasinë e shumë njerëzve e kaloi pengesën e rezistencës së biznesit dhe paralajmëroi kushte dhe rregulla rigoroze për përpunimin e të dhënave personale të qytetarëve të BE-së. Motivin dhe qëllimin e kësaj rregullative, shumica e shohin në zhvillimin e teknologjive të reja, në digjitalizimin dhe globalizmin, ku të dhënat personale janë ato që i lëvizin këto procese. Republika e Maqedonisë së Veriut, në procesin e harmonizimit të legjislacionit së saj me legjislacionin e BE-së, më datë 24.02.2020 e shndërroi Rregullativën e përgjithshme për mbrojtjen e të dhënave personale (GDPD), në ligj të saj kombëtar për mbrojtjen e të dhënave personale (lex generalis)[2]. Në këtë mënyrë, edhe njëherë theksohet rëndësia e të drejtës së mbrojtjes së të dhënave personale, si pjesë e të drejtave dhe lirive themelore të qytetarëve dhe si vlerë thelbësore të çdo shoqërie moderne dhe të zhvilluar teknologjikisht.

Ligji për mbrojtjen e të dhënave personale (në tekstin e mëtejmë: LMDHP) zbatimin e saj material e gjen në çdo situatë që nënkupton përpunimin e të dhënave personale të qytetarëve të Republikës së Maqedonisë së Veriut, pa marrë parasysh nëse personi fizik respektivisht juridik i cili e bën përpunimin është nga sektori privat, shtetëror ose civil, ndërkaq duke u nisur nga koncepti i garantimit të privatësisë dhe integritetit personal të individit. Përjashtim ekziston vetëm për ato përpunime të të dhënave personale që bëhen nga personat fizik, për aktivitete personale, respektivisht aktivitete në shtëpi.

Institucionet shtetërore dhe publike nevojitet që t'i zbatojnë këto rregulla për mbrojtjen e të dhënave personale, pavarësisht nëse aktivitetet e përpunimit të të dhënave personale të personave fizikë është në formë të shkruar ose elektronike. Në institucione shtetërore dhe publike, bëjnë pjesë të gjitha organet e shtetërore dhe lokale dhe organet e tjera shtetërore të themeluara në pajtim me Kushtetutën dhe ligjin, institucionet që kryejnë veprimtari nga sfera e arsimit, shkencës, shëndetësisë, kulturës, punës, mbrojtjes sociale dhe mbrojtjes së fëmijëve, sportit dhe veprimtari të tjera me interes publik, të përcaktuara me ligj (agjenci, fonde, institucione publike dhe ndërmarrje publike të themeluara nga Republika e Maqedonisë së Veriut ose nga komunat, nga Qyteti i Shkupit si dhe nga komunat e Qytetit të Shkupit). Në Këto raste, është e detyrueshme që të caktohet oficer për mbrojtjen e të dhënave personale, pa marrë parasysh llojin dhe vëllimin e të dhënave personale që përpunohen.

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj (General Data Protection Regulation 2016/6792 - GDPR)

[2] Ligji për mbrojtjen e të dhënave personale („Gazeta zyrtare e RMV-së, nr. 42 nga data 16.02.2020)

3. QËLLIMI

Qëllimi i këtij Udhëzuesi është që të japë udhëzime dhe rekomandime praktike për zbatimin e rregullave aktive nga sfera e të dhënave personale nga institucionet shtetërore dhe publike, në rolin e kontrollorëve si dhe për oficerët për mbrojtjen e të dhënave personale, që janë të emëruar nga ana e tyre. Për të kuptuar më mirë atë, është i domosdoshëm një lexim paraprak të Ligjit për mbrojtjen e të dhënave personale dhe të akteve nënligjore përkatëse.

Duke u udhëhequr nga rregullativa evropiane dhe praktikat më të mira ndërkombëtare dhe vendore nga kjo sferë, ky Udhëzues jep udhëzime praktike, për atë se çfarë nevojitet të miratohet dhe zbatohet nga ana e kontrollorëve dhe përpunuesve gjatë aktiviteteve për përpunimin e të dhënave personale, në drejtim të kuptimit dhe zbatimit më të lehtë të dispozitave nga rregullativa relevante, duke minimizuar rrezikun e keqpërdorimit eventual, si dhe duke marrë parasysh edhe teknologjitë dhe zgjidhjet më të reja teknologjike.

Gjithashtu, ky Udhëzues në veçanti është i dedikuar për të ndihmuar personat e caktuar në pozitën e Oficerit për mbrojtjen e të dhënave personale, duke siguruar hapa të detajuara dhe shembuj praktikë për realizimin më të thjeshtë të detyrave, përgjegjësive dhe sfidave të tij, në pajtim me rregullat e zbatueshme nga kjo sferë.

Për këtë qëllim, ky Udhëzues është i ndarë në katër pjesë:

- **PJESA 1**, jep një pasqyrë të dispozitave ligjore që kanë të bëjnë me caktimin e oficerit për mbrojtjen e të dhënave personale si dhe me kualifikimet e nevojshme për emërimin e kësaj pozite të punës;
- **PJESA 2**, i sqaron në mënyrë të detajuar detyrat e punës së oficerëve, obligimet e kontrollorëve dhe përpunuesve, të ndjekura me shembuj praktikë nga praktika e mirë vendore dhe ndërkombëtare, veçanërisht në aspekt të përvojave pozitive të zbatimit të deritanishëm të Rregullativës së përgjithshme për mbrojtjen e të dhënave personale, në pjesën e ofrimit të shërbimeve publike elektronike të të dhënave personale.
- **PJESA 3**, e sqaron zbatimin dhe ndikimin e inteligjencës artificiale (në tekstin e mëtejmë: IA) mbi të drejtat e njeriut dhe
- **PJESA 4**, janë Shtojcat e këtij Udhëzuesi ku janë dhënë shembujt e formularëve dhe materialeve ndihmëse për zbatimin e tyre gjatë punës së përditshme.

4. PËRKUFIZIME

Përkufizimi i termave është në pajtim me Ligjin për mbrojtjen e të dhënave personale dhe shërben për t'i qartësuar bazat mbi të cilat bazohet e drejta e mbrojtjes së të dhënave personale, edhe atë:

- **Të dhëna personale** janë çdo informatë në lidhje me personin e identifikuar fizik ose personin fizik që mund të identifikohet drejtpërdrejt ose tërthorazi me ndihmën e identifikuesit. Shembull për të dhënat personale janë: emri dhe mbiemri, NVAQ, lokacioni, IP adresa, identiteti online, posta elektronike, shprehitë e shpenzimit, informatat bankare, etj.
- **Kategori e veçantë e të dhënave personale** janë ato të dhëna të cilat paska më tepër e prekin privatësinë e personave fizikë, siç janë: prejardhja racore ose etnike, qëndrimet politike, bindjet fetare ose filozofike ose pjesëmarrja në organizatat sindikale, si dhe të dhënat gjenetike, të dhënat biometrike, të dhëna për shëndetin ose të dhënat për jetën seksuale ose orientimin seksual të personit fizik.
- **Subjekti i të dhënave personale** është personi fizik të dhënat e të cilit janë duke u përpunuar.
- **Përpunimi i të dhënave personale** është çdo aktivitet që realizohet mbi të dhënat personale, në mënyrë automatike dhe mënyra të tjera, siç janë: mbledhja, evidentimi, organizimi, strukturimi, ruajtja, aftësimi ose ndryshimi, tërheqja, konsultimi, kontrolli, përdorimi, zbulimi përmes transferimit, publikimit ose në mënyrë tjetër disponueshmërisë së tyre, harmonizimi ose kombinimi, kufizimi, fshirja ose shkatërrimi.
- **Qëllimi i përpunimit** është arsyeja për të cilën përpunohen të dhënat personale për përmbushjen e obligimit ligjor, marrëveshjes ose realizimin e punëve me interes publik.
- **Aktiviteti i përpunimit të të dhënave personale** është çdo aktivitet individual i punës për kryerjen e të cilit janë të domosdoshme të dhënat personale. Shembuj të këtyre aktiviteteve për përpunimin e të dhënave personale janë: pagesa e rrogës, evidenca e kohës së punës, lidhja e kontratës së punësimit, shënimi i punonjësit të ri në aplikacionin e resurseve njerëzore, lëshimin e lejeve dhe vërtetimeve, përllogaritja e tatimit dhe shpenzimeve të tjera publike, regjistrimi i nxënësve në shkollë fillore dhe të mesme, sigurimi i mbrojtjes shëndetësore, etj.

Si veprimtari primare e kontrollorit konsiderohen aktivitetet kryesore të cilat janë të nevojshme për arritjen e qëllimeve të kontrollorit, me ç'rast veprimtaria primare nuk është e domosdoshme që të jetë vetëm ajo që ka të bëjë me përpunimin e të dhënave personale, por edhe aktivitetet e tjera që parashohin përpunimin

e të dhënave personale (p.sh ofrimi i shërbimeve nga sfera e komunikimeve elektronike, profilizimi, ndjekja e vendndodhjes përmes aplikacioneve celulare, ndjekja e të dhënave për shëndetin përmes aplikacioneve celulare, etj.). Këto shembuj kanë të bëjnë me ndjekjen e rregullt dhe sistematike të subjekteve të të dhënave personale, respektivisht të të gjitha formave të ndjekjes dhe profilizimit përmes internetit, që termi-ndjekje nuk është i kufizuar vetëm në ambientin virtual.

Gjegjësisht, me zhvillimin e teknologjisë dhe IA-së gjithnjë e më shumë aktualizohet edhe çështja e IAs-së. Edhe krahas aspekteve pozitive që i bart me vete ky zhvillim, megjithatë, veçanërisht gjatë të shkruarit e Rregullativës (ligjore dhe nënligjore), pritet që t'u kushtohet vëmendje e posaçme edhe të drejtave të njeriut, sundimit të së drejtës dhe etikës, nëse shfrytëzohet IA-ja në proceset e punës të institucioneve.

Në aspekt të organeve të pushtetit shtetëror, përdorimi i IA-së dhe teknologjive themelore kanë ndikim të tyre në aspekt të spektrit të gjerë të sferave, përfshirë shëndetësinë, arsimin, zbatimin e rregulloreve dhe përgjegjësinë shoqërore. Në këtë drejtim, imponohen një sërë çështjesh që nevojitet të shqyrtohen, sepse IA-ja ka potencial për t'i cenuar pikërisht të drejtat e njeriut dhe për t'i minuar ligjet që i mbrojnë ata.

Përpunimi i një numri të madh të të dhënave, në kombinim me IA-në, mund ta cenojë të drejtën e privatësisë, për shkak të ekzistimit të rrezikut të mbikëqyrjes dhe monitorimit të shtuar të individëve. Personat që kanë qasje në teknologjinë që e mundëson IA-ja mund të kërkojnë shënime publike dhe të dhëna tjera të disponueshme dukshëm më shpejtë se sa që do të ishte e mundshme pa e shfrytëzuar teknologjinë.

5. AGJENCIA PËR MBROJTJEN E TË DHËNAVE PERSONALE (AMDHP)

Agjencia për Mbrojtjen e të Dhënave Personale është organ i pavarur kompetent për mbikëqyrjen e ligjshmërisë për aktivitetet e ndërmarra gjatë përpunimit të të dhënave personale në territorin e Republikës së Maqedonisë së Veriut si dhe për mbrojtjen e të drejtave dhe lirive themelore të personave fizikë në aspekt të përpunimit të të dhënave të tyre personale.

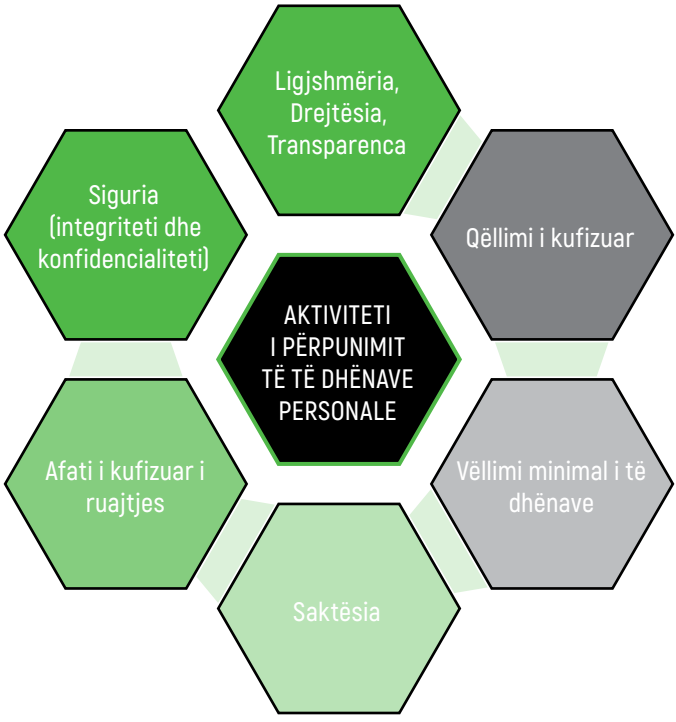
Qëllimi kryesor i Agjencisë është forcimi, promovimi dhe mbrojtja e privatësisë së të dhënave të personave fizikë përmes realizimit të mbikëqyrjes, dhënies së udhëzimeve, si dhe mendimeve në pajtim me rregullat ligjore.

6. PARIMET LIDHUR ME PËRPUNIMIN E TË DHËNAVE PERSONALE DHE ZBATIMI I TYRE

Ligji për mbrojtjen e të dhënave personale lejon përpunimin e të dhënave personale, nëse gjatë përpunimit janë zbatuar gjashtë parimet e përcaktuara[3].

Pasi të përcaktohen në mënyrë precize dhe të detajuar të gjitha aktivitetet për përpunimin e të dhënave personale në kuadër të institucionit, atëherë hapi i radhës është që të zbatohen këto parime për secilin aktivitet në veçanti.

Kontrollorët janë të detyruar që të veprojnë në pajtim me parimet për mbrojtjen e të dhënave personale.



6.1. Ligjshmëria, drejtësia dhe transparenca

Të dhënat personale mund të përpunohen vetëm nëse ekziston bazë ligjore[4] për përpunim dhe në mënyrë që është e drejtë dhe transparente ndaj subjektit të të dhënave personale, të dhënat e të cilit përpunohen.

[3] Neni 9 paragrafi 1 nga Ligji për mbrojtjen e të dhënave personale („Gazeta zyrtare e RMV-së" numër 42 nga data 16.2.2020)

[4] Neni 10 nga Ligji për mbrojtjen e të dhënave personale („Gazeta zyrtare e RMV-së" numër 42 nga data 16.2.2020)

6.1.1. Ligjshmëria

Që të mund të zbatohet aktiviteti i përpunimit të të dhënave personale, patjetër duhet të ekzistojë bazë ligjore për atë përpunim. Ndërkaq, ligjshmëria nuk nënkupton domosdoshmërisht se përpunimi duhet të jetë në pajtim me ndonjë ligj konkret, siç edhe mendojnë shumica prej nesh por se përpunimi i të dhënave personale guxon që të realizohet vetëm sipas rregullave të caktuara që i përcakton LMDHP-ja. Megjithëse ekzistojnë gjashtë lloje të bazave ligjore, vetëm pesë prej tyre janë të zbatueshme për sektorin publik, edhe atë:

6.1.1.1. Obligimi ligjor:

Aktiviteti i përpunimit të të dhënave personale i cili nevojitet që institucioni të përmbush obligim ligjor, është ai aktivitet që ligjshmërinë e tij do ta gjejë në nenin 10 paragrafi 1 alineja 3 e Ligjit. Nëse për një aktivitet konkret në Evidencën e aktiviteteve të përpunimit konstatohet baza ligjore, më tutje është më lehtë të njihen edhe aktivitetet të cilat institucioni bazë ligjore që t'i ndërmarrë.

Shembuj:

- Përpunimi i të dhënave për pagesë të pagës për të punësuarit, sepse institucioni ka obligim ligjor që të punësuarve t'u paguaj paga dhe atë obligim nuk mund ta përmbushë pa i përpunim paraprak të të dhënave të tyre personale.
- Përpunimi i të dhënave personale nga ana e qendrës kompetente për punë sociale ka bazë ligjore (Ligji për mbrojtje sociale[5]) që shfrytëzuesit potencial të ndihmës së garantuar minimale t'ia përpunojë të dhënat personale siç janë emri, mbiemri, adresa e vendbanimit, vendlindja, NVAQ, arsimi, statusi i punës, shtetësia, përkatësia etnike, numri i letërnjoftimit, etj.

6.1.1.2. Përmbushja e marrëveshjes:

Përpunimi është i nevojshëm për përmbushjen e marrëveshjes ku njëra palë është subjekti i të dhënave personale, ose për të ndërmarrë aktivitete me kërkesë të subjektit të të dhënave personale para lidhjes së marrëveshjes (neni 10 paragrafi 1 alineja 2 e Ligjit). Në atë drejtim, nëse aktiviteti del nga marrëveshja, atëherë përpunimi i të dhënave personale patjetër duhet të përfshihet me ndonjë bazë tjetër juridike.

Shembuj të aktivitetit i cili ligjshmërinë e tij e gjen në këtë bazë:

- Përpunimi i biografisë personale të dorëzuar pas konkursit të shpallur për punësim, si aktivitet që i paraprinë marrëveshjes për punësim (pa marrë parasysh që ai mund edhe të mos lidhet për shkak të moszgjedhjes së kandidatit).
- Përpunimi i të dhënave personale (emri, mbiemri, adresa dhe NVAQ) për lidhjen e marrëveshjes për prokurim publik, ku bartësi është person fizik.

[5] „(Gazeta zyrtare e RMV-së, nr.104 nga data 23.5.2019")

6.1.1.3. Mbrojtja e jetës ose interesit thelbësor:

Përpunimi është i nevojshëm për mbrojtjen e interesave thelbësore të subjektit të të dhënave personale ose të një personi tjetër fizik.

Kjo bazë juridike shfrytëzohet në situata të rralla, kur aktiviteti i përpunimit me të dhënat personale mund të nevojitet për shpëtimin e jetës së dikujt, që më së shpeshti është e lidhur me nevojën për sigurimin e ndihmës urgjente mjekësore.

Shembull:

- Përpunimi i letërnjoftimit ose një dokumenti tjetër për identifikimin e një personi pa ndjenja, me qëllim që t'i jepet ndihma e para ose leja e vozitjes për ta parë grupin e gjakut

6.1.1.4. Realizimi i punëve me interes publik ose me autorizim publik:

Përpunimi nevojitet për realizimin e punëve me interes publik ose gjatë realizimit të autorizimit publik të kontrollorit, të përcaktuar me Ligj.

Shembull:

- Për regjistrimin e nxënësve në shkollat e mesme, në pajtim me Ligjin për arsimin e mesëm, mblidhen të dhënat personale si emri dhe mbiemri i nxënësit, data dhe vendlindja, adresa dhe vendbanimi, vendlindja, gjinia, emri dhe mbiemri i prindërve ose kujdestarëve.
- Për qëllime të aplikimit për bursa, Ministria e Arsimit dhe Shkencës, krahas emrit dhe mbiemrit, adresës së vendbanimit të studentit, i mbledh edhe të dhënat e nënshtetësisë, xhirollogarisë, si dhe suksesit të arritur të nxënësve.

6.1.1.5. Pëlqimi:

Subjekti i të dhënave personale ka dhënë pëlqim për përpunimin e të dhënave të tij personale për një ose më shumë qëllime konkrete. Pëlqimi patjetër duhet të jetë dhënë lirshëm, qartë dhe të mund të tërhiqet lehtë, andaj kontrollorët duhet të kenë kujdes që gjithmonë kur si bazë juridike e përpunimit të të dhënave personale shfrytëzohet pëlqimi i dhënë (nuk lejohen më praktikat me shënim automatik të fushave për pëlqim).

Shembull:

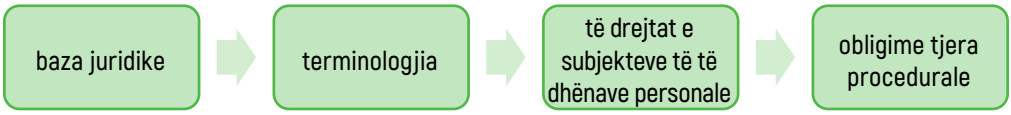
- Përpunimi i të dhënave në një institucion për publikimin e fotografive lejohet nëse ka pëlqim të qartë nga subjekti/prindi/kujdestari i të dhënave personale me qëllim të publikimit të fotografive të fëmijëve nga institucioni edukativo-arsimor.

Vëmendje: *Në aspekt të bazës juridike nga pika 5.1.1, gjatë harmonizimit të legjislacionit sektorial me Ligjin për mbrojtjen e të dhënave personale, Agjencia për Mbrojtjen e të Dhënave Personale ka miratuar Vendim për përcaktimin e metodologjisë për harmonizimin e legjislacionit sektorial*[6]*.*

[6] („Gazeta zyrtare e RMV-së nr.38 nga 21.2.2022")

Në këtë drejtim, hapi i parë i ministrive kompetente është kontrollimi dhe identifikimi nëse një ligj i caktuar ka të bëjë me mbledhjen, përpunimin, ruajtjen, shfrytëzimin dhe dorëzimin e të dhënave personale, respektivisht nëse përfshin çfarëdo aktivitete për përpunimin e të dhënave personale. Rekomandohet që të identifikohen ligjet relevante ekzistuese që duhet të ndryshohen (ndryshohen dhe plotësohen) që të njëjtat edhe më tutje të harmonizohen me dispozitat e Ligjit për mbrojtjen e të dhënave personale. Në rast të përgatitjes së ligjeve të reja në të cilat ka aktivitete për përpunimin e të dhënave personale, përgjegjësia për harmonizimin e zgjidhjes së re ligjore është e ministrisë e cila e propozon atë ligj.

Me qëllim të vlerësimit nëse janë përmbushur kërkesa të caktuara që dalin nga Ligji për mbrojtjen e të dhënave personale, për kontrollimin e ligjeve të reja dhe atyre ekzistuese, që kanë të bëjnë me përpunimin e të dhënave personale, mund të shërbejnë kriteret në vijim:



1. Baza juridike e përpunimit

- Përpunimi i të dhënave personale është i ligjshëm, vetëm edhe derë në atë shkallë nëse për atë ka bazë juridike për përpunim (p.sh. përmbushja e obligimit ligjor, realizimi i punëve me interes publik ose gjatë realizimit të autorizimeve publike, etj.)

2. Përshtatja e terminologjisë

- Termet që përdoren në ligjet ekzistuese duhet të përshtaten me terminologjinë e Ligjit për mbrojtjen e të dhënave personale, në mënyrë që të sigurohet konsistencë juridike (p.sh. Përdorimi i termit "përpunim" për t'i përkufizuar të gjitha operacionet ose përmbledhjen e operacioneve që kryhen mbi të dhënat personale).

3. Të drejtat e subjekteve të të dhënave personale

- Përcaktim i kufizimeve të të drejtave të subjekteve drejtpërdrejt në vetë ligjin dhe me përmbushjen e kërkesave të caktuara nga Ligji për mbrojtjen e të dhënave personale (kufizim i arsyetuar për shkak të nevojës për sigurimin e një ose më tepër qëllimeve dhe dispozita ligjore që e përcakton kufizimin)

4. Obligime të tjera procedurale

- Kontrollim nëse ligji aktual përmban dhe nëse nevojiten që të inkorporohen dispozita konkrete ligjore (p.sh. Obligim për fshirje, korrigjim ose kufizim të përpunimit). Obligimet e këtilla duhet të realizohen me detyrë zyrtare nga ana e organeve publike, sepse ai obligim ekziston pa marrë parasysh faktin nëse subjekti i të dhënave personale ka kërkuar ose jo realizimin e të drejtës së tyre për fshirjen e të dhënave personale.

6.1.1.6. Interesi legjitim

Përpunimi i cili bazohet në interesin legjitim të kontrollorit, **nuk është i zbatueshëm për sektorin publik.** Në përgjithësi, kjo bazë përkufizohet si një interes zyrtar i kontrollorit për të kryer aktivitet të caktuar të përpunimit të të dhënave personale dhe ky interes mbizotëron mbi të drejtat dhe liritë e subjekteve, të dhënat personale të të cilave janë prekur me aktivitetin e përpunimit.

Kur organizata shfrytëzon interes legjitim si bazë ligjore për përpunim, ajo duhet doemos të realizojë një test të balancimit, respektivisht të konstatojë nëse aktiviteti i përpunimit është i domosdoshëm që organizata të funksionojë/ta realizojë veprimtarinë e saj, respektivisht nëse aktiviteti i përpunimit mund të konsiderohet se nuk mbizotëron mbi të drejtat dhe liritë e subjektit të të dhënave personale. Nëse me përgjigjet e këtyre pyetjeve dëshmohet se mbizotëron mbi interesat ose të drejtat dhe liritë themelore të subjektit, atëherë organizata nuk mund ta shfrytëzojë interesin legjitim si bazë ligjore për përpunimin.

Që një aktivitet të jetë ligjor, mjafton të realizohet një prej bazave të theksuara ligjore. Praktikë e zakonshme e gabuar është që të kërkohet pëlqim nga subjektet e të dhënave personale edhe krahas asaj që ekziston bazë tjetër ligjore për aktivitetet e përpunimit të të dhënave personale.

6.1.2. Drejtësia

Drejtësia, respektivisht përpunimi i drejtë nënkupton se subjekti i të dhënave personale patjetër duhet të jetë i vetëdijshëm për faktin se të dhënat e tij personale janë duke u përpunuar, ta di qëllimin e përpunimit dhe se si ato të dhëna mblidhen, ruhen dhe shfrytëzohen, që do t'i mundësojë të sjellë një vendim të informuar nëse pajtohet me atë përpunim (në rastet kur përpunimi është i bazuar në pëlqim) dhe se ka mundësi t'i shfrytëzojë të drejtat e tij për mbrojtjen e të dhënave personale[7].

6.1.3. Transparenca

Jotransparenca, gjatë përpunimit të të dhënave personale, historikisht njihet si një prej rreziqeve më të mëdha ndaj privatësisë së personave fizik. Organizata të ndryshme për nevojat e tyre mbledhin të dhëna të ndryshime, pa e informuar personin fizik, se për cilin qëllim mblidhen të dhënat e tij personale, si përpunohen, si ruhen, etj.

E lidhur ngushtë me drejtësinë, transparenca nënkupton se institucionet patjetër duhet të jenë të hapura dhe të qarta ndaj subjekteve të të dhënave personale, para se të fillohet me përpunimin e të dhënave të tyre personale. Për shembull, me prezantimin e njoftimit për privatësi, politikës së privatësisë, politikës së

[7] Kreu IX i këtij Udhëzuesi.

përdorimit të skedarëve, etj., me çka subjekti do të njoftohet me detajet e përpunimit para se t'i japë të dhënat e tij personale.

P.sh. Krijimi i Politikës së privatësisë me të cilën do të parashihen të dhënat e përgjithshme për përpunimin e të dhënave personale për vizitën e një faqeje zyrtare të internetit dhe/ose për shfrytëzimin e shërbimeve të caktuara administrative përmes të njëjtës, për të realizuar detyrat dhe autorizimet ligjore.

Faqja e internetit dhe formularët e tillë duhet të japin qartë informata për atë se si subjektet e të dhënave personale mund t'i realizojnë të drejtat e tyre (përfshirë edhe publikimin e qartë dhe publik me të dhëna kontaktuese për Oficerin - edhe pse ajo nuk duhet domosdo të përfshijë emrin dhe mbiemrin e oficerit);

6.2. Kufizimi i qëllimit

Të dhënat personale duhet të mblidhen vetëm për qëllime konkrete, të qarta dhe legjitime dhe ato nuk guxojnë të jenë pjesë e përpunimit, në mënyrë që nuk është në pajtim me këto qëllime. Prapë se prapë, përpunimi i mëtejmë i të dhënave personale për qëllimet e arkivimit me interes publik, për hulumtime shkencore dhe historike dhe për qëllime statistikore, në pajtim me nenin 86 paragrafi (2) nga LMDHP, nuk konsiderohet si joadekuat, në pajtim me qëllimin inicial të përpunimit.

6.3. Vëllimi minimal i të dhënave

Përpunimi i të dhënave personale patjetër duhet të jetë adekuat, relevant dhe i kufizuar, vetëm në atë që është e domosdoshme për arritjen e qëllimeve të atij përpunimi dhe në atë drejtim nëse qëllimi i përpunimit nuk mund të arrihet në ndonjë mënyrë tjetër të arsyeshme.

6.4. Saktësia

Kontrollorët patjetër duhet të sigurohen se të dhënat personale janë të sakta dhe sipas nevojës, të përditësohen, përmes hapave/masave të caktuara për fshirje, respektivisht korrigjim të të dhënave të pasakta personale, pa pasur nevojë të prolongimit dhe në pajtim me qëllimin e përpunimit. Konkretisht kontrollorët duhet që saktë t'i shënojnë informatat që i mbledhin ose marrin, së bashku me burimin e atyre informatave.

6.5. Afati i kufizuar i ruajtjes

Të dhënat personale duhet të ruhen në formën e cila lejon identifikimin e subjekteve të të dhënave personale, për periudhën e nevojshme për qëllimet për të cilat përpunohen. Në këtë drejtim, nevojitet që kontrollorët të parashohin afat kohor për fshirjen e të dhënave personale ose për revizion periodik. Gjatë përkufizimit të afatit të ruajtjes, kontrollori fillimisht duhet të sigurohet nëse ekzistojnë afate të përcaktuara ligjore për ruajtjen e të dhënave personale, e nëse jo, patjetër duhet t'i përcaktojë afatet me rregulla të tij të brendshme.

6.6. Siguria (integriteti dhe konfidencialiteti)

Të dhënat personale duhet të përpunohen në mënyrë e cila siguron siguri dhe konfidencialitet adekuat të tyre, përfshirë edhe mbrojtjen nga qasja e paautorizuar ose joligjore ose shfrytëzimin e të dhënave personale dhe pajisjeve të përpunimit, si dhe nga humbja, shkatërrimi ose dëmtimi i rastësishëm, duke zbatuar masa adekuate teknike dhe organizative.

Kontrollorët janë përgjegjës për harmonizimin me të gjitha parimet e lartpërmendura për mbrojtjen e të dhënave personale, në drejtim të ndërmarrjes së përgjegjësisë për përpunimin e tyre të të dhënave personale dhe harmonizimin me LMDHP-në, për të demonstruar harmonizim dhe që të kenë mundësi që ta dëshmojnë të njëjtën, përfshirë edhe para AMDHP-së, duke prezantuar evidencën dhe zbatimin e masave adekuate.

7. LLOGARIDHËNIA

Llogaridhënia[8] paraqet një prej risive në rregullativën ligjore. Me rëndësi të veçantë është që të kuptohet rëndësia e termit të llogaridhënies të cilin ligji e përshkruan si obligim të kontrollorit që të punojë sipas parimeve që kanë të bëjnë me përpunimin e të dhënave personale, si dhe detyrë për ta dëshmuar të njëjtën.

Thënë ndryshe, llogaridhënia më së miri do të përshkruhej si një përmbledhje e obligimeve me të cilat duhet të harmonizohet institucioni, që të ketë mundësi për ta treguar dhe dëshmuar harmonizimin me rregullativën e zbatuar për mbrojtjen e të dhënave personale. Pikërisht llogaridhënia si kërkesë ligjore, na sugjeron se rruga e një institucioni deri në harmonizimin e plotë të punës së tij me Ligjin për mbrojtjen e të dhënave personale dhe me aktet relevante nënligjore nuk është e njëhershëm por paraqet një proces të pandërprerë, i cili ka edhe fillim të vet dhe është objekt i përplotësimit të vazhdueshëm. Arsyeja e tij është se Ligji nuk "kërkon" të harmonizohet institucioni, por të harmonizohet mënyra e punës që nënkupton implementimin e rregullave të veprimit që mundësojnë mbrojtjen e të dhënave personale, që shfrytëzohen dhe përpunohen në proceset e punës së institucionit.

Miratimi dhe implementimi i thjeshtë i procedurave dhe politikave të brendshme, ose kompletimi formal i formularëve/deklaratave të caktuara, më nuk mjaftojnë që një institucion të konsiderohet si i harmonizuar me rregullativën e zbatueshme, por duhet doemos të punohet për vendosjen e rregullave thelbësore të veprimit, rritjen e vetëdijes dhe më atë edhe ndërtimin e një kulture për mbrojtjen e të dhënave personale nga të gjithë faktorët e përfshirë.

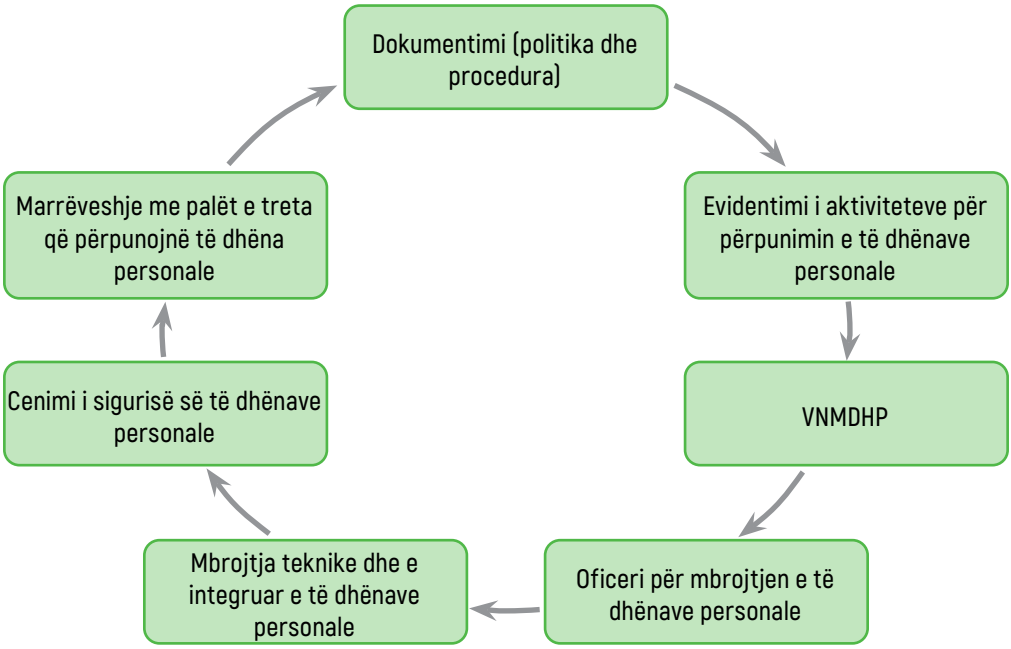
7.1. Demonstrimi i llogaridhënies

Demonstrimi i llogaridhënies nga institucionet publike parasheh disa faza të cilat në mënyrë grafike mund të prezantohen në këtë mënyrë:

7.1.1. Dokumentacioni (Përpilimi i politikave dhe procedurave të cilat i përfshijnë aktivitetet e përpunimit)

Dokumentacioni luan një rol të konsiderueshëm në risitë lidhur me llogaridhënien. Ajo i mundëson kontrollorit dhe/ose përpunuesit të të dhënave personale që ta garantojë dhe ta tregojë harmonizimin me obligimet e tija, si dhe me hapat e ndërmarrë për të.

[8] Neni 9 paragrafi 2 nga Ligji për mbrojtjen e të dhënave personale („Gazetë zyrtare e RMV-së" nr. 42 nga data 16.02.2020)



Sigurimi i dokumentacionit parasheh disa aspekte siç është evidenca e aktiviteteve të përpunimit, vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale, evidenca për cenimin e sigurisë së të dhënave personale, si dhe masat e ndërmarra korrigjuese, procedurat që kanë të bëjnë me realizimin e të drejtave, marrëveshjeve me përpunuesit dhe personat e jashtëm prej të cilëve shfrytëzohen shërbimet, mjetet e mbikëqyrjes së transmetimeve jashtë Bashkimit Evropian, analiza me shkrim e oficeri për mosekzistimin e konfliktit të interesave, etj.

Dokumentacioni si mjet thelbësor jep një pasqyrë të detajuar të aktiviteteve të realizuara të përpunimit të të dhënave personale dhe mundëson që të planifikohet menaxhimi i tyre. Për këto arsye, nevojitet që dokumentacioni të ruhet, respektivisht të sigurohet se e njëjta është relevante, respektivisht se është lëndë e përditësimit të rregullt.

7.1.2. Evidenca e aktiviteteve për përpunimin e të dhënave personale

Lidhur me mbajtjen e evidencës për aktivitetet e përpunimit, ajo paraqet obligim të kontrollorit, respektivisht përpunuesit të të dhënave personale.

Përmes evidencës realizohet ndjekja e aktiviteteve të realizuara për përpunimin e të dhënave personale, duke i mundësuar oficerit kontroll të plotë të aktiviteteve për përpunimin dhe si rrjedhojë edhe mundësi për propozimin e masave, që nevojiten për mbikëqyrjen e tyre të rregullt.

7.1.3. Vlerësimi i ndikimit ndaj mbrojtjes së të dhënave personale (VNMDHP)

Me realizimin e VNMDHP-së, aty ku nevojitet, institucionet publike do ta demonstrojnë llogaridhënien me dokumentimin efektiv dhe me shqyrtimin e përpunimeve të cilët mund të rezultojnë me një rrezik të lartë për të drejtat dhe liritë e personave fizikë.

7.1.4. Oficeri për mbrojtjen e të dhënave personale

Emërimi i oficerit për mbrojtjen e të drejtave personale është një prej mënyrave se si institucioni publik e demonstron llogaridhënien e tij.

7.1.5. Mbrojtja e të dhënave personale by design dhe by default

Kjo qasje natyrshëm do t'i çojë institucionet publike deri në një llogaridhënie dhe harmonizim. Mbrojtja e të dhënave personale by design dhe by default nënkupton se e drejta e privatësisë është marrë parasysh në çdo hap të përpunimit – që nga mbledhja e të dhënave personale e deri te fshirja e tyre eventuale.

7.1.6. Cenimi i sigurisë së të dhënave personale

Ruajtja e shënimeve për cenimet e sigurisë së të dhënave personale dhe aty ku është e nevojshme raportimi i cenimit të sigurisë së të dhënave personale është gjithashtu mënyrë se si demonstrohet llogaridhënia.

7.1.7. Marrëveshjet me palët e treta të cilët përpunojnë të dhëna personale

Lidhja e marrëveshjeve me organizatat që përpunojnë të dhëna personale në emër të institucionit, pa marrë parasysh nëse bëhet fjalë për raportin kontrollor me kontrollor, kontrollor me përpunues ose kontrollorë të përbashkët.

Llogaridhënia si e tillë është një proces i pandërprerë. Masat që i keni zbatuar patjetër duhet që të rishikohen rregullisht dhe sipas nevojës edhe të përditësohen. Llogaridhënia mund t'ju ndihmojë që të ndërtoni besim te subjektet e të dhënave personale dhe mund t'ju ndihmojë gjatë mbikëqyrjes nga Agjencia për Mbrojtjen e të Dhënave Personale.

8. TË DREJTAT E SUBJEKTEVE TË TË DHËNAVE PERSONALE

Subjektet e të dhënave personale i kanë këto të drejta:

- Të drejtën e informimit;
- Të drejtën e qasjes;
- Të drejtën e korrigjimit;
- Të drejtën e fshirjes;
- Të drejtë për kufizim të përpunimit;
- Të drejtën e transferimit;
- Të drejtën e ankesës;
- Të drejtën që të mos jetë objekt i miratimit të automatizuar të vendimeve individuale dhe profilizimit;
- Të drejtën e parashtrim të kërkesës në Agjencinë;

8.1. E drejta e informimit

Sipas ligjit, subjekti i të dhënave personale ka të drejtë që të informohet për identitetin e kontrollorit, të dhënat e tij kontaktuese, qëllimin e përpunimit, bazën ligjore të përpunimit dhe informata të tjera relevante që janë të domosdoshme për të siguruar përpunim të drejtë dhe transparentë të të dhënave personale.

P.sh: Njoftimi për privatësi, politikat e privatësisë, etj.

8.2. E drejta e qasjes

Çdo subjekt i të dhënave personale mund të kërkojë informatë nga kontrollori nëse përpunohen të dhënat e tij dhe nëse përpunohen të marrë qasje në të dhënat personale edhe atë: për qëllimet e përpunimit, kategoritë e të dhënave personale që përpunohen, shfrytëzuesit ose kategoritë e shfrytëzuesve të cilëve u janë zbuluar ose do t'u zbulohen të dhënat personale, veçanërisht shfrytëzuesit nga vende të treta ose organizata ndërkombëtare, afati i paraparë i ruajtjes së të dhënave personale, ekzistimi i se drejtës për të kërkuar fshirjen ose korrigjimin e të dhënave personale nga kontrollori ose kufizimi i përpunimit të të dhënave personale lidhur me subjektin e të dhënave personale, ose e drejta e ankesës kundër atij përpunimi, e drejta e parashtrimit të kërkesës në AMDHP-në, kur të dhënat personale nuk mblidhen nga subjekti i të dhënave personale, të gjitha informatat e disponueshme për burimin e tyre dhe ekzistimin e një procesi të automatizuar të vendimmarrjes, përfshirë edhe profilizimin. Kontrollori duhet t'i

përgjigjet. Kontrollori është i obliguar që të sigurojë kopje të të dhënave personale të cilat përpunohen. Nëse subjekti i të dhënave personale parashtron kërkesë në formë elektronike, subjektit të të dhënave personale informatat do t'i sigurohen në mënyrë të zakonshme që shfrytëzohet në rast të formës elektronike, përveç nëse subjekti i të dhënave personale nuk ka kërkuar më ndryshe.

8.3. E drejta e korrigjimit

Me kërkesë të subjektit të të dhënave personale, kontrollori është i obliguar që të plotësojë, ndryshojë ose fshijë të dhënat personale ose ta ndërpresë përpunimin e të dhënave personale, në rastet kur ato janë të paplota, të pasakta ose të vjetruara, ose nëse përpunimi është joligjor.

Pa marrë parasysh faktin nëse subjekti i të dhënave personale ka parashtruar kërkesë personale, në momentin kur konstaton se të dhënat personale janë të paplota, të pasakta ose të vjetruara, kontrollori është i obliguar që t'i plotësojë, ndryshojë ose fshijë.

Afati për korrigjim është **15 ditë** nga dita e parashtrimit të kërkesës.

8.4. E drejta e fshirjes

Subjekti i të dhënave personale ka të drejtë që të kërkojë nga kontrollori që t'i fshijë të dhënat e tij personale, nëse është përmbushur një prej kushteve në vijim:

- Të dhënat personale më nuk janë të nevojshme për qëllimet për të cilat janë mbledhur;
- Nëse përpunimi është bazuar në pëlqim, ndërsa subjekti i të dhënave personale e ka tërhequr pëlqimin;
- Subjekti i të dhënave personale ka parashtruar ankesë kundër përpunimit;
- Të dhënat personale janë përpunuar në mënyrë joligjore;
- Të dhënat personale duhet të fshihen si rezultat i obligimit ligjor të kontrollorit;
- Të dhënat personale janë mbledhur në lidhje me shërbime të shoqërisë informatike për fëmijë.

Nëse kontrollori i ka publikuar të dhënat personale për të cilat është kërkuar që të fshihen (p.sh. Mediat sociale), patjetër duhet të ndërmerren masa racionale për t'i informuar të gjitha palët e tjera që në ndërkohë i kanë marrë ato të dhëna personale për t'i përpunuar si kontrollorë, me qëllim të realizimit të së drejtës për fshirje.

Kontrollori mund ta refuzojë kërkesën e subjektit të të dhënave personale për

të fshirë të dhënat e tij, nëse përpunimi nevojitet për të realizuar të drejtën e lirisë së shprehjes dhe informimit, për harmonizimin e kontrollorit me një obligim ligjor, ose për realizimin e punëve me interes publik, mes tjerash edhe shëndetin publik, si dhe për qëllime të arkivimit me interes publik, për hulumtime shkencore, historike ose statistikore.

Afati për korrigjim është **30 ditë** nga dita e parashtrimit të kërkesës.

Vërejtje: Kontrollori duhet doemos që për këtë kërkesë t'i njoftojë palët e treta (shfrytëzuesit) të cilëve u janë dhënë të dhënat konkrete personale për shfrytëzim.

8.5. E drejta e kufizimit të përpunimit

Subjekti i të dhënave personale ka të drejtë që të kërkojë kufizimin e përpunimit të të dhënave të tij personale nëse:

- Saktësia e të dhënave personale është kontestuar nga ana e subjektit (përpunimi do të kufizohet deri sa të kontrollohet saktësia e të dhënave);
- Përpunimi është joligjor, ndërsa subjekti kundërshton që të fshihen të dhënat personale;
- Kontrollori më nuk ka nevojë për të dhënat personale për arsye se qëllimi i përpunimit të tyre është përmbushur, ndërsa subjekti kërkon që të ruhen për realizimin e kërkesave të tij ligjore;
- Subjekti i të dhënave personale ka parashtruar kundërshtim për përpunimin dhe deri sa pritet verifikimi se cilat interesa mbisundojnë (interesat legjitime të kontrollorit kundrejt interesave të subjekteve) përpunimi kufizohet.

Vërejtje: Kushti i fundit për këtë të drejtë nuk është i zbatueshëm për institucionet publike sepse interesi legjitim si bazë ligjore nuk është i zbatueshëm për institucionet publike.

8.6. E drejta e transferimit

Ligji i jep të drejtë subjektit të të dhënave personale për t'i marrë të dhënat e tija personale në një format të strukturuar, dhe i përdorur në mënyrë të zakonshme dhe në një format të lexueshëm makinerik. Gjithashtu, subjekti i të dhënave personale ka të drejtë që këto të dhëna personale t'i transferojë te kontrollor tjetër, pa pengesa nga ana e kontrollorit prej të cilit kërkohet transferimi. Kushtet për shfrytëzimin e kësaj të drejte janë:

- Ai ia ka dhënë të dhënat personale kontrollorit,
- Përpunimi bëhet në bazë të pëlqimit ose në bazë të një obligimi kontraktues ose

- Përpunimi bëhet në mënyrë të automatizuar.

8.7. E drejta e kundërshtimit

Nëse të dhënat personale të subjektit përpunohen në bazë të interesit publik të kontrollorit, përfshirë edhe profilizimin dhe marketingun e drejtpërdrejtë, subjekti ka të drejtë të parashtrojë kundërshtim kundër atij përpunimi. Kontrollori si përgjigje ndaj kundërshtimit duhet doemos ta ndërpresë përpunimin, përveç nëse nuk dëshmohet se interesi i tij mbizotëron mbi interesat, të drejtat dhe liritë e subjektit të të dhënave personale.

Vërejtje: Kjo e drejtë duhet doemos t'i bëhet me dije subjektit në mënyrë të qartë, ndaras si informatë prej informatave të tjera që i jepen në njoftimin për privatësi, politikën e privatësisë etj.

8.8. E drejta që të mos jetë objekt i miratimit të automatizuar të vendimeve individuale dhe profilizimit

Kjo e drejtë ka të bëjë vetëm me ato vendime që bazohen veçanërisht në përpunimin dhe profilizimin automatik, e që shkaktojnë pasoja juridike ose në mënyrë të ngjashme ndikojnë mbi subjektin e të dhënave personale. Kontrollori do ta refuzojë këtë kërkesë nëse vendimi i cili është objekt i përpunimit automatik:

- nevojitet për lidhjen ose realizimin e marrëveshjeve ndërmjet subjektit të të dhënave personale dhe kontrollorit;
- lejohet me ligj që zbatohet në aspekt të kontrollorit ose
- bazohet në pëlqimin e shqiptuar të subjektit të të dhënave personale.

8.9. E drejta e parashtrimit të kërkesës në Agjencinë për Mbrojtjen e të Dhënave Personale

Secili subjekti i të dhënave personale ka të drejtë që të parashtrojë kërkesë në Agjencinë, nëse konsideron se përpunimi i të dhënave personale i shkel dispozitat e këtij ligji, me këtë rast duke mos e vënë në pikëpyetje cilat do mjete tjera administrative ose gjyqësore për mbrojtje juridike.

Lidhur me këto të drejta, oficeri për mbrojtjen e të dhënave personale është i ngarkuar për realizimin e të drejtave të subjekteve të të dhënave personale dhe për përmbushjen e obligimeve të kontrollorit.

9. MARKETINGU I DREJTPËRDREJTË

Marketingu shpeshherë e tejkalon kufirin e privatësisë, me çka në veçanti merret ligji i ri LMDHP. Çdo blerje moderne, kërkon mbledhjen e të dhënave personale të caktuara dhe përfshin aktivitete në drejtim të zbulimit të qëllimeve dhe shprehive të konsumatorëve, me qëllim që të përshtatet oferta.

Marketingu i drejtpërdrejtë përfshin çdo komunikim të realizuar përmes cilado mjeteve për prezantim të materialit të marketingut ose reklamimit, në drejtim të përpunimit të të dhënave të një personi të caktuar fizik. Në këtë drejtim, ky komunikim më së shpeshti përfshin dorëzimin e letrave të personalizuara me postë, kontaktimin përmes telefonit, postës elektronike, SMS, dritareve (pop-ap), por edhe mënyrave të tjera. Sikurse për çdo përpunim të të dhënave personale, ashtu edhe për qëllimet e marketingut, duhet doemos të ekzistojë një bazë relevante ligjore, e cila mund të merret përmes sigurimit të pëlqimit të drejtpërdrejtë nga ana e subjektit të të dhënave personale.

Gjatë përpunimit të të dhënave personale për qëllimet e marketingut të drejtpërdrejtë, kontrollori duhet doemos të veprojë sipas rregullave nga Ligji për mbrojtjen e të dhënave personale, respektivisht:

- të ekzistojë bazë ligjore për përpunim (pëlqim nga subjekti i të dhënave personale);
- informatë subjektit të të dhënave personale për përpunimin e të dhënave personale për qëllimet e marketingut (parimi i transparencës);
- zbatimi i masave adekuate teknike dhe organizative për mbrojtjen e të dhënave personale, përfshirë edhe përgjigjen me shkrim me dispozitat e detyrueshme që lidhen me përpunuesin, i cili do të bëjë marketing të drejtpërdrejtë në emër të kontrollorit (p.sh. agjencitë e marketingut);
- të mos bëhet transferimi jashtë BE-së/hapësirës ekonomike evropiane, përveç nëse përmbushen kushtet ligjore (dispozitat e përputhshmërisë) që lejojnë që të bëhet ky transferim dhe
- Kërkesa të tjera nga Ligji për mbrojtjen e të dhënave personale.

Vërejtje: Rekomandohet që gjatë përgatitjes së Deklaratës për pëlqim, ajo të jetë e veçantë për këtë qëllim konkret, përkatësisht të mos jetë pjesë e dhënies së përgjithshme të pëlqimeve për qëllime të ndryshime, p.sh. dhënies së përgjithshme të pëlqimeve për qëllime të ndryshme, p.sh. Përpunimi automatik (profilizimi) fotografimi etj.

E drejta e tërheqjes (eng. opt out) të deklaratës së dhënë për pëlqim të përpunimit

të të dhënave personale për qëllime të marketingut të drejtpërdrejtë, duhet t'i mundësohet subjektit të të dhënave personale. Për mënyrën se si mund ta tërheq pëlqimin, subjekti informohet paraprakisht (përmes politikës së privatësisë, njoftimit për privatësi, politikës së skedarëve, etj.) me ç'rast tërheqja duhet të bëhet në mënyrë të lehtë dhe të thjeshtë, duke shfrytëzuar kanalet e komunikimit që janë në dispozicion, si dhe pa shpenzime shtesë.

Rekomandohet që kontrollori të parashohë një evidencë sistematike (ekzistojnë mjete, modele dhe zgjidhje të ndryshme softuerike) për pëlqime të dhëna dhe të tërhequra për përpunim, për qëllimet e marketingut direkt që do t'u mundësojë një pasqyrë të përditësuar të gjendjes në çdo kohë.

Shembull: Organet e pushtetit shtetëror mund të bazohen në kriterin "gjatë zbatimit të kompetencave të tyre", por ajo nuk nënkupton se çështja e marketingut të drejtpërdrejtë nuk vendoset asnjëherë në raport me sektorin publik, p.sh. siç është dorëzimi i postës elektronike të qytetarëve për evenimente kulturore, duke shfrytëzuar të dhënat personale nga Regjistri i popullsisë.

10. OFICERI PËR MBROJTJEN E TË DHËNAVE PERSONALE

10.1. Caktimi i Oficerit për mbrojtjen e të dhënave personale

Në pajtim me nenin 41, paragrafi 1 i LMDHP-së, nevojitet që të caktohet Oficer për mbrojtjen e të dhënave personale në rastet në vijim:

- nëse jeni organ i administratës shtetërore;
- kur veprimtaria juaj themelore përbëhet nga aktivitete për përpunim të vëllimshëm të cilët imponojnë ndjekje të rregullt dhe sistematike të personave fizikë (p.sh, kompania e sigurimit e cila ka sistem për videombikëqyrje në disa qendra tregtare); dhe
- kur veprimtaria juaj themelore përfshin përpunim të vëllimshëm të kategorive të posaçme të të dhënave personale (p.sh. të dhëna biometrike, të dhëna gjenetike, të dhëna shëndetësore) ose të dhëna lidhur me aktgjykimet ndëshkuese dhe veprat penale (p.sh. aktivitetet për përpunimin e të dhënave spitalore konsiderohen si përpunim i vëllimshëm kundrejt përpunimit që e bën mjeku, për një individ, e që nuk llogaritet si përpunim i vëllimshëm i të dhënave personale).

Sipas të lartpërmendurës, obligimi për emërimin e Oficerit ka të bëjë me të gjitha organet shtetërore, me përjashtim të gjykatave, por vetëm kur veprojnë në kuadër të kompetencave të veta. Kjo nënkupton se megjithatë gjykatat janë të obliguara

që të caktojnë oficer për mbrojtjen e të dhënave personale që do të kujdeset për harmonizimin me rregullat për mbrojtjen e të dhënave personale, në aspekt të aktiviteteve për përpunimin e të dhënave personale që janë jashtë kompetencave të tyre gjyqësore.

Ndërkaq, Oficeri për mbrojtjen e të dhënave personale ka obligim për fshehtësi dhe konfidencialitet gjatë realizmit të detyrave të tij.

Gjithashtu, nevojitet që në faqen zyrtare të internetit të institucionit, të publikohen detajet për kontakt me oficerin për mbrojtjen e të dhënave personale, ndërsa ato duhet të dorëzohen edhe në Agjencinë për mbrojtjen e të dhënave personale.

10.2. Kualifikime të nevojshme

Në pajtim me LMDHP-në gjatë emërimit të një punonjësi në pozitën e oficerit për mbrojtjen e të dhënave personale, nevojitet që të plotësohen njohurit dhe kualifikimet e përcaktuara profesionale, në mënyrë që personi të emërohet në këtë funksion.

Për shkak të natyrës së aktiviteteve, nga Oficeri në mënyrë plotësuese pritet që të posedojë edhe një sërë aftësish personale dhe interpersonale. Nga ato personalet duhet të ketë: integritet, iniciativë, organizim, diskrecion, durim, interes dhe motivim për realizimin e këtij funksioni, si dhe një nivel të lartë të etikës profesionale, zhvillim të shkathtësive për zbatimin e praktikave konkrete duke imponuar ndryshime sipas nevojës, si dhe aftësi për bartje të njohurive dhe pozitë të qartë, si dhe afirmim të pozitës sipas nevojës;

Në aspekt të shkathtësive interpersonale, nga Oficeri pritet që të mund ta ruaj komunikimin e mirë me të gjitha palët e inkuadruar, si dhe të posedojë aftësi për negociata dhe zgjidhje të konflikteve.

Veprimi i oficerit për mbrojtjen e të dhënave personale nuk guxon të shkaktojë konflikt të interesave, duke realizuar detyra të tjera, sepse në atë mënyrë do të vihet në pikëpyetje realizimi i pavarur i detyrave dhe obligimeve të tij (përfshirë edhe ndikimet e mundshme politike dhe jo vetëm, gjatë realizimit të detyrave të tij), e as që guxon njëkohësisht të jetë i punësuar që merr pjesë në përcaktimin e qëllimeve dhe mënyrave të përpunimit të të dhënave personale (pa marrë parasysh faktin nëse bëhet fjalë për pozita të larta menaxhuese ose pozita më të ulëta të punës).

Për shembull: Për OMDHP nuk mund të emërohet drejtuesi i kontrollorit/ përpunuesit, e as administruesi i sistemit informatik.

Ligjit për mbrojtjen e të dhënave personale parasheh mundësi që organet e administratës shtetërore të përcaktojnë për disa organe në përbërje të organit kompetent, që të ketë vetëm një oficer për mbrojtjen e të dhënave personale,

me kusht që ai të jetë në dispozicion për secilin institucion. Ky oficer mund të angazhohet në bazë të kontratës në vepër për të siguruar ato shërbime.

Grupi i punës 29 (WP29) i Këshillit Evropian për mbrojtjen e të dhënave personale në dokumentin e tyre – "Udhëzime për oficerët për mbrojtjen e të dhënave personale"[9], thekson si në vijim:

- në rast të një organi shtetëror ose publik, oficeri për mbrojtjen e të dhënave personale duhet të ketë njohur solide të rregullave dhe procedurave (të brendshme) administrative në kuadër të organizatës.

10.3. Roli i oficerit për mbrojtjen e të dhënave personale

Oficeri për mbrojtjen e të dhënave personale paraqet lojtar kryesor në sistemin për menaxhimin e të dhënave personale. Misioni që i është dhënë oficerit për mbrojtjen e të dhënave personale e konfirmon rolin e tij të rëndësishëm për ndjekjen e procesit dinamik në nivel më të lartë të harmonizimit nga sfera e mbrojtjes së të dhënave personale dhe pozitës së tij (me garanci për pavarësinë e tij nga udhëheqësia) në institucionin, prej të cilit pritet që të balancohet ndërmjet interesave të institucionit dhe të drejtave të subjekteve të të dhënave personale.

Oficeri për mbrojtjen e të dhënave personale ka rol këshillues dhe revizionues të kontrollorit, e ndjek harmonizimin e punës së organit shtetëror me rregullat relevante dhe bën edukimin e vazhdueshëm të punonjësve nga sfera e mbrojtjes së të dhënave personale.

Për këto arsye nevojitet që në kohë dhe në mënyrë adekuate të përfshihet në të gjitha aspektet e sferës së mbrojtjes së të dhënave personale.

Revokimi/shkarkimi i bartësit të funksionit – oficerit për mbrojtjen e të dhënave personale është i arsyeshëm, vetëm nëse personi nuk i përmbush më kushtet për realizmin e detyrave dhe obligimeve të punës.

[9] Guidelines on Data Protection Officers ('DPOs') (wp243rev.01)https://ec.europa.eu/newsroom/article29/items/612048

11. DETYRAT DHE PËRGJEGJËSITË E OFICERIT PËR MBROJTJEN E TË DHËNAVE PERSONALE

Gjatë përshkrimit të detyrave të punës nga sfera e mbrojtjes së të dhënave personale, në dokumentin juridik (vendim, aktvendim, etj.), për emërimin tuaj në pozitën – oficer për mbrojtjen e të dhënave personale, nevojitet që organi/ institucion shtetëror të udhëhiqet nga ato që janë përcaktuar me Ligjin për mbrojtjen e të dhënave personale:

Shembull: Përshkrimi i detyrave të punës të OMDHP-së

Detyra pune të OMDHP-së
❖ Kujdeset për implementimin e rregullave për mbrojtje të të dhënave personale dhe akteve të brendshme të miratuara nga kontrollori ❖ Zhvillon strategji për mbrojtje të të dhënave personale e cila është adekuate me kontrollorin konkret ❖ Udhëheq me njësinë organizative për mbrojtjen e të dhënave personale – nëse është vendosur ❖ E përfaqëson kontrollorin (interne dhe publike) për çështje nga sfera e mbrojtjes së të dhënave personale
Në nivel operativ: ❖ Kujdeset për informim të subjekteve të të dhënave personale për të drejtat e tyre, si dhe kontrollori për obligimet e tij që dalin nga rregullat për mbrojtjen e të dhënave personale; ❖ Kujdeset për rritjen e vetëdijes te kontrollori për mbrojtje të të dhënave personale ❖ Organizon dhe realizon trajnime për të punësuarit që janë përfshirë në operacionet e përpunimit të të dhënave personale; ❖ E ndjek harmonizimin dhe respektimin e rregullave për mbrojtje të të dhënave personale nga kontrollori, përmes identifikimit dhe vlerësimit të kërkesave ligjore, vlerësimit të tyre dhe zhvillimit të udhëzimeve për përmbushje të tyre nga kontrollori; ❖ I përgatit aktet e brendshme të kontrollorit dhe e ndjek harmonizimin e tyre me rregullat për mbrojtje të të dhënave personale; ❖ E ndjek zbatimin e masave teknike dhe organizative për sigurim të sigurisë dhe fshehtësisë gjatë përpunimit të të dhënave personale te kontrollori ❖ E këshillon dhe i jep rekomandime adekuate kontrollorit në drejtim të përmbushjes së obligimeve që dalin nga rregullat për mbrojtje të të dhënave personale; ❖ Është përfshirë në mënyrë aktive në të gjitha projektet që kanë të bëjnë me implementimin e sistemeve të TI-së ose krijimin e produkteve dhe serviseve të reja, që në fazat e hershme të projektit me qëllim të dizajnimit të sistemeve ose produkteve në përputhje me parimet themelore për mbrojtje të të dhënave personale;

- Është përfshirë në mënyrë aktive në krijimin dhe zbatimin e proceseve që përfshijnë përpunim të të dhënave personale;
- Kryen kontrolle lidhur me respektimin e rregullave për mbrojtje të të dhënave personale në bazë të rregullave të paracaktuara për zbatimin e tyre.
- Jep këshilla në aspekt të vlerësimit të ndikimit të operacioneve të planifikuara të përpunimit mbi mbrojtjen e të dhënave personale dhe ndjekjes së kryerjes së këtij vlerësimi (Data Protection Impact Assessment);
- Realizon mbledhje të rregullta me nivelin më të ulët të udhëheqjes/menaxhmentit lidhur me çështjet nga sfera e mbrojtjes së të dhënave personale;
- Bashkëpunon dhe vepron si pikë kontakti për DMDHP (i ofron mbështetje DMDHP-së gjatë zbatimit të obligimeve ligjore dhe bashkëpunon me DMDHP-në në drejtim të zhvillimit dhe promovimit të praktikave më të mira për tema konkrete)
- E koordinon komunikimin e kontrollorit në procedurat që udhëhiqen para Drejtësisë për Mbrojtje të të Dhënave Personale
- Realizon kontakte me subjektet e të dhënave personale dhe kujdeset për zbatimin e procedurës dhe përgjigjen në kohë ndaj kërkesave dhe kundërshtimeve të tyre drejtuar kontrollorit, e në lidhje me çështje nga sfera e mbrojtjes së të dhënave personale;
- E koordinon komunikimin e brendshëm për çështje nga sfera e mbrojtjes së të dhënave personale, duke vepruar si pikë e vetme e kontaktit dhe e koordinon mbështetjen e jashtme të dhënë nga shoqëritë këshillimore, të avokatit dhe shoqëritë tjera juridike.

Funksionet, respektivisht detyrat e oficerit për mbrojtjen e të dhënave personale mund në përgjithësi të grupohen në katër kategori kryesore, edhe atë: kategori preliminare, organizative, këshilluese dhe të revizionit.

Përmes këtyre hapave për kontroll të realizimit të detyrave dhe përgjegjësive tuaja, do të keni mundësi që në mënyrë të thjeshtë të keni qasje në atë se çfarë pritet nga pozita e juaj e punës – oficer për mbrojtjen e të dhënave personale. Gjithashtu, përmes shembujve konkrete të praktikës do të mund të qaseni dhe t'i implementoni suksesshëm detyrat dhe obligimet e Tuaja.

11.1. Funksioni preliminar:

Si fillim, nevojitet që të bëhet regjistrimi i të gjitha të dhënave personale që i posedoni dhe të dokumentohet se pse janë të nevojshme të dhënat personale që përpunohen. Në këtë drejtim, duhet të përcaktohet ambienti i kontrollorit dhe të hartëzohen aktivitetet për përpunimin e të dhënave personale të organizatës, në korniza më të gjëra.

Gjegjësisht, do të keni mundësi që në mënyrë profesionale t'i realizoni detyrat tuaja, vetëm nëse jeni të njoftuar me:

(i) shpërndarjen e brendshme dhe shpërndarjen e detyrave dhe përgjegjësive, në aspekt të çfarëdo përpunimi të të dhënave personale, në kuadër të institucionit Tuaj;

(ii) raportet dhe marrëveshjet e jashtme të institucionit me institucionet/trupat e tjerë (bashkëpunimi me institucione të tjera, shfrytëzimi i shërbimeve nga furnizuesit e jashtëm dhe palë të treta, shfrytëzimi i shërbimeve cloud, etj.); dhe

(iii) korniza(t) juridike, me të cilat rregullohen detyrat tuaja.

Gjatë realizimit të këtyre aktiviteteve, nevojitet që të dokumentoni si vijon:

- Si janë marrë të dhënat personale?
- Pse ruhen të dhënat personale?
- A nevojiten ende të dhënat personale?
- A janë të sigurta të dhënat personale?
- Me kë ndahen të dhënat personale?

Tjetër çfarë duhet të bëni është që të bëni përcaktimin e qëllimeve të përpunimit dhe të garantoni siguri të përpunimit, përmes zbatimit të masave adekuate teknike dhe organizative.

Në këtë fazë, mund të vijë deri te përputhja e aktiviteteve nga kjo detyrë me aktivitetet që kanë të bëjnë me realizimin e evidentimit të aktiviteteve për përpunimin e të dhënave personale në Detyrën 1 nga Funksioni organizativ – por në këtë fazë, nevojitet që aktivitetet e përpunimit të të dhënave personale të identifikohen thjeshtë, në aspekt të qëllimit të përpunimit dhe teknologjive të përpunuara.

Në këtë mënyrë, do të merrni ide fillestare për atë se cilat detyra dhe përgjegjësi i ka secila njësi organizative (sektor, shërbim, departament ose seksion), në lidhje me aktivitetet e përpunimit të të dhënave personale dhe njëkohësisht do ta identifikoni "pronarin e procesit zyrtar" të secilit përpunim të të dhënave personale.

Në bazë të rezultateve të fituara, do të krijoni një shteg të lëvizjes së të dhënave personale në kudër të institucionit tuaj, me qëllim për të siguruar kontroll më të madh të përpunimit të tyre në kuadër të aktiviteteve të punës së institucionit.

Shembull:

- Regjistri Qendror (Ligji për Regjistrin Qendror);[10]
- Regjistri i sanksioneve të shqiptuara ndëshkuese (Ligji për zbatimin e sanksioneve);[11]
- Regjistri për ndalime për realizim të veprimtarisë dhe Regjistri i dënimeve të personave juridikë (Ligji për kundërvajtje);[12]
- Regjistri i tatimpaguesve (Ligji për procedurë tatimore);[13]
- Regjistri i pedofilëve (Ligji për regjistër të posaçëm të personave të dënuar me aktgjykime të plotfuqishme për vepra penale të keqpërdorimit seksual të personave të mitur dhe pedofili);[14]
- Regjistri i shfrytëzuesve të ndihmës sociale (Ligji për mbrojtje sociale);[15]
- Regjistri i librave amë zyrtare (Ligji për evidencë amë);[16]
- Regjistri i pronës së paluajtshme (Ligji për tatimin e pronës) etj.[17]

Në formë qendrore elektronike, një pjesë e këtyre të dhënave të qytetarëve shkëmbehen edhe në mënyrë interoperabile nga ana e institucioneve të ndryshme përmes Regjistrit Qendror të popullsisë (Ligjit për menaxhim elektronik dhe shërbime elektronike[18], ku është përcaktuar shkëmbimi elektronik i të dhënave dhe mënyra se si ajo duhet të realizohet, ofrimi i shërbimeve elektronike, puna e ndërmjetësuesve, si dhe Ligjit për regjistrin qendror të popullsisë[19] dhe Ligjit për dokumente elektronike, identifikim elektronik dhe shërbime konfidenciale[20])

Pyetjet e shumta që do të dalin nga kjo fazë preliminare nuk duhet që patjetër menjëherë të adresohen dhe zgjidhen – por nevojiten që në mënyrë adekuate të shënohen aktivitetet e përpunimit të të dhënave personale të institucionit në

---

[10] Ligji për regjistrin qendror („Gazeta zyrtare e Republikës së Maqedonisë" numër 50/2001, 49/2003, 109/2005, 88/2008, 35/11, 43/14, 199/14, 97/15, 153/15, 27/16, 83/18 dhe 311/20)

[11] Ligji për ekzekutimin e sanksioneve („Gazeta zyrtare e Republikës së Maqedonisë së Veriut" nr. 99/19, 220/19 dhe 236/22)

[12] Ligji për kundërvajtjet („Gazeta zyrtare e Republikës së Maqedonisë së Veriut" nr. 96/19)

[13] Ligji për procedurë tatimore („Gazeta zyrtare e Republikës së Maqedonisë" бpoj 13/2006, 88/2008, 159/2008, 105/2009, 133/2009, 145/10, 171/10, 53/11, 39/12, 84/12, 187/13, 15/15, 97/15, 129/15, 154/15, 23/16 и 35/18 и „Gazeta zyrtare e Republikës së Maqedonisë së Veriut" бpoj 275/19, 290/20 dhe 247/22)

[14] Ligji për regjistër të veçantë për persona të dënuar me aktgjykim të plotfuqishëm për vepra penale për keqpërdorim seksual të personave të mitur dhe pedofili („Gazeta zyrtare e Republikës së Maqedonisë"nr. 11/2012 dhe 112/2014)

[15] Ligji për mbrojtje sociale („Gazeta zyrtare e Republikës së Maqedonisë së Veriut " numër 104/19, 146/19, 275/19, 302/20, 311/20, 163/21, 294/21, 99/22, 236/22 dhe 65/23)

[16] Ligji për evidencë amë („Gazeta zyrtare e Republikës së Maqedonisë" nr. 8/1995; 38/2002; 66/2007; 98/2008; 67/2009; 13/2013 dhe 43/2014)

[17] Ligji për tatimet e pronës ("Gazeta zyrtare e Republikës së Maqedonisë" nr. 61/04, 92/07, 102/08, 35/11, 53/11, 84/12, 188/13, 154/15, 192/15, 23/16 dhe 151/21)

[18] Ligji për menaxhim elektronik dhe shërbime elektronike ("Gazeta zyrtare e RMV" nr. 98 dhe nr. 244)

[19] Ligji për regjistrin qendror të popullsisë ("Gazeta zyrtare e RMV" nr. 98/19 dhe 275/19)

[20] Ligji për dokumente elektronike, identifikim elektronik dhe shërbime konfidenciale ("Gazeta zyrtare e RMV" nr. 101/19 dhe 275/19)

kuptimin më të gjerë, si një hap kryesor drejt krijimit të një regjistri të këtyre aktiviteteve me të gjitha aktivitetet individuale të përpunimit të të dhënave personale, të realizuara në kuadër të detyrës së radhës.

Vërejtje: *Oficeri për mbrojtjen e të dhënave personale në këtë fazë është në rolin e koordinatorit të personave përgjegjës të sektorëve kompetent dhe personit këshillues i cili ka rol për të udhëhequr në procesin e harmonizimit me rregullativën e kësaj sfere.*

11.2. Funksioni organizativ:

Detyra 1: Përgatitja e evidencës (regjistrit) të aktiviteteve për përpunimin e të dhënave personale

Në pajtim me nenin 34 të LMDHP-së, çdo kontrollor, respektivisht përpunues duhet doemos "të mbaj" evidencë për aktivitetet e përpunimit, duke theksuar detajet e ndryshme për secilin aktivitet, siç është titulli i kontrollorit dhe personi i autorizuar, oficeri për mbrojtjen e të dhënave personale, titulli i procesit të punës, qëllimi(et) e përpunimit, kategoritë e subjekteve të të dhënave, kategoritë e të dhënave personale, transmetimi nga vende të treta (nëse ka), afatet për fshirje, përshkrimi i përgjithshëm i masave teknike dhe organizative dhe kategoritë e shfrytëzuesve që janë të zbuluar ose që do t'i zbulojnë të dhënat personale.

Kjo detyrë për të mbajtur evidencë të aktiviteteve të përpunimit të të dhënave personale është e lidhur ngushtë me parimin e transparencës, që e lehtëson edhe mbikëqyrjen efektive nga ana e Agjencisë për Mbrojtjen e të Dhënave Personale.

Sipas kësaj, evidenca është parakusht për harmonizim, si dhe masë efikase për llogaridhënie.

Çdo kontrollor dhe përpunues duhet të obligohet që të bashkëpunojë me organin mbikëqyrës dhe me kërkesë të tij, t'i vendos në dispozicion shënimet, respektivisht evidencën.

Shënimi që mbahet paraqet mjet që i mundëson kontrollorit dhe organit mbikëqyrës, që të kenë qasje në aktivitetet e përpunimit të të dhënave personale të cilat i realizon një institucion.

Në Shtojcën nr.1 të këtij Udhëzuesi, mund të gjeni edhe propozim-formularë për Evidencë (Regjistër) për përpunimin e të dhënave personale (të njëjtat nuk janë të obligueshme, por do të ndihmonin gjatë krijimit të Evidencës tuaj të aktiviteteve për përpunimin e të dhënave personale dhe shënimeve adekuate).

Vërejtje: *Nëse ekziston çfarëdo dyshimi lidhur me nevojën për evidentim, kontrollori duhet të kërkojë këshill nga Ju, ndërsa juve ju rekomandohet që gjatë dhënies së këshillës, ajo të jetë në drejtim të mbajtjes së evidencës, sesa të rrezikoni se institucioni të mos veprojë në pajtim me nenin 34 të LMDHP-së.*

Vërejtje:

1. Në pyetjen nëse evidenca e aktiviteteve për përpunimin e të dhënave personale nevojitet që të jetë publike (në internet ose në formë tjetër) ose jo, mund ta shihni më hollësisht në Detyrën 2, "Pasqyra e aktiviteteve për përpunimin e të dhënave personale ".

2. Krijimi i evidencës si e tillë ende nuk e përfshin edhe vlerësimin e harmonizimit të aktiviteteve të evidentuara për përpunimin e të dhënave personale: ajo është bërë në Detyrën 2 – por kuptohet, evidenca duhet të jetë objekt i ndryshimit dhe përditësimit të rregullt, respektivisht gjithmonë kur do të bëhen ndryshime në aktivitetet e përpunimit të të dhënave personale, të shënuara në të.

Detyra 2: Pasqyra e aktiviteteve për përpunimin e të dhënave personale

Shumica e institucioneve të sektorit publik ofrojnë një spektër të gjerë të shërbimeve. Kjo nënkupton se ato zakonisht ruajnë dhe ndajnë sasi të mëdha të të dhënave personale që duhet të jenë lëndë e përpunimit të përgjegjshëm. Të dhënat janë kryesore si për atë se si institucionet e sektorit publik ofrojnë shërbime për qytetarët, i përmirësojnë sistemet dhe proceset e tyre dhe me këtë sjellin vendime të mira. Megjithatë, ekziston një mungesë e besimit, kur bëhet fjalë për menaxhimin e të dhënave personale nga sektori publik, veçanërisht në aspekt të shërbimeve elektronike publike, për shkak të numrit të madh të hakimeve për të cilat ishim dëshmitarë në periudhën e kaluar.

Evidenca e aktiviteteve për përpunimin e të dhënave personale përfshin edhe informata për qëllimet e përpunimit, kategoritë e subjekteve të të dhënave personale, kategoritë e të dhënave personale dhe marrësve e të dhënave personale, bartjen e të dhënave personale, afatin për fshirjen e të dhënave personale, si dhe masat teknike dhe organizative që zbatohen.

Ky lloj i evidencës është një mënyrë e shkëlqyeshme për vendosjen e kontrollit ndaj përpunimit dhe lëvizjes së të dhënave personale, në kuadër të organizatës suaj. Ruajtja e këtyre informatave në një vend e lehtëson dëshminë për harmonizim me Ligjin për mbrojtjen e të dhënave personale.

Pasi ta keni përgatitur evidencën e aktiviteteve për përpunimin e të dhënave personale në organizatën tuaj (Detyra 1), hapi i radhës është që të realizoni një kontroll të thellë të këtyre aktiviteteve për përpunimin e të dhënave personale, për të parë nëse janë plotësuar kushtet nga LMDHP-ja, lidhur me:

- përcaktimin e qëllimit të përpunimit dhe të kufizimeve;
- vlefshmëria e secilit pëlqim dhe dëshmisë së dokumentuar për atë ose për zbatimin e cilësdo bazë ligjore për përpunim (vlefshmëria përcaktohet në bazë të ekzistimit të bazës ligjore për përpunimin e të dhënave personale, në pajtim me nenin 10 paragrafi (1) i LMDHP-së)

Vërejtje: Keni parasysh se nëse bazoheni në pëlqime, të siguruara nga personat fizikë, si bazë ligjore për përpunimin e të dhënave personale, atëherë duhet të garantoni se janë plotësuar të gjitha kushtet e përcaktuara me ligj.

Vërejtje: Nëse përpunimi i të dhënave personale, nga ana tjetër përfshin kategori të posaçme të të dhënave personale (p.sh. të dhëna biometrike, të dhëna gjenetike, të dhëna shëndetësore etj.), duhet të thirreni në bazën ligjore të përpunimit, si dhe në njërën prej përjashtimeve për përpunimin e të dhënave të tilla, të dhënë me nenin 13 të LMDHP-së;

- rëndësia dhe domosdoshmëria e të dhënave të përpunuara personale, në aspekt të qëllimit(eve) të përcaktuara;
- cilësia e të dhënave (saktësia, përditësimi, etj. i të dhënave si dhe minimizimi dhe anonimizimi i tyre);
- informata dorëzuar subjektit të të dhënave personale (kur të dhënat mblidhen nga subjekti i të dhënave personale, ose me kërkesë të subjektit të të dhënave personale, p.sh. të dhënat e mbledhura në bazë të pëlqimit të tij për shfrytëzimin e skedarëve, si vizitues i një faqeje interneti)

Vërejtje: Në këtë drejtim, prej juve pritet që t'i informoni subjektet në kuadër të politikës tuaj për privatësi/njoftime për privatësi/deklarata për privatësi për:

- periudha kohore në të cilën të dhënat personale ruhen në formë e cila mund të identifikohet;
- siguria teknike, organizative dhe fizike e të dhënave (përfshirë edhe qasjen fizike, kufizimet e qasjeve (emri i përdoruesit, fjalëkalimet, politikat, etj.), enkriptimi, etj.;
- transferimi ndërkufitar i të dhënave (juridike, kontraktuese ose raporte të tjera); etj.

Sipas të lartpërmendurës, padyshim se do të keni mundësi që të vlerësoni nëse aktiviteti konkret i përpunimit të të dhënave personale, në tërësi është në pajtim me parimet e ligjshmërisë dhe drejtësisë.

Krijimi i një Evidence të saktë dhe mirëmbajtja e saj e përditësuar me aktivitetet e përpunimit të të dhënave personale, që paraqet një hartë të të dhënave personale në një institucion, njëkohësisht është dokument i dobishëm për institucionin me të cilin do të kontribuohet për mbrojtjen më të madhe të të dhënave personale.

Siç e theksuam paraprakisht, nuk ekziston një formë e paraparë e evidencës. Por sipas natyrës së saj të "ndryshimit", më praktike do të jetë që të ruhet në formë elektronike duke shfrytëzuar ndonjërën prej pakove MS Office ose ndoshta ndonjë softuer të posaçëm për këtë qëllim.

Në aspekt të masave teknike dhe organizative, në pajtim me nenin 28 të LMDHP-së, kontrollori është i obliguar që të zbatojë masa të tilla për sigurim që i përgjigjen

nivelit të sigurisë që është adekuat për rreziqet ndaj lirive dhe të drejtave të personave fizikë. Këtu mund të parashihen masa të ndryshme për përballje me këto rreziqe, si p.sh: pseudonimizimi/enkriptimi, dispozitat standarde për fshehtësi, masa teknike për të siguruar fshehtësi, integriteti, qasja në sistemet dhe mundësia për kthimin e të dhënave, etj. Megjithatë, kjo ofron një kontroll parësor nga aspekti i asaj nëse masat e ndërmarra janë "adekuate" me "state of art", shpenzimet për implementimin e natyrës, vëllimin, kontekstin dhe qëllimet e përpunimit, si dhe probabilitetin dhe seriozitetin për paraqitje të rrezikut ndaj të drejtave dhe lirive të personave fizikë".

LMDHP-ja nuk kërkon nga kontrollorët që ta publikojnë evidencën e aktiviteteve për përpunimin e të dhënave personale të një institucioni. Mirëpo, LMDHP-ja gjithashtu nuk e ndalon atë.

Në përgjithësi, ekzistojnë shumë arsye se pse evidenca e aktiviteteve duhet të jetë publike:

- kontribuon për transparencë;
- ndihmon në forcimin e besimit të publikut;
- e lehtëson shkëmbimin e njohurive;
- mospublikimi do të ishte hap prapa pas rregullave të vjetra.

Kjo të paktën, është e rëndësishme për ne si institucione shtetërore. Mbetet mundësia, që legjislacioni kombëtar të imponojë obligimin për publikim të evidencës.

Në këtë drejtim, nëse konsideroni se aktivitetet e përpunimit të të dhënave personale nuk janë të harmonizuara me kërkesat rregullatorë, nevojitet që ta njoftoni pa prolongim personin përgjegjës (pronarin) e procesit zyrtar, për mungesat dhe të propozoni masa adekuate për zbutje (nëse nevojitet dhe tërësisht ta ndërpresë përpunimin e mëtejmë të këtyre të dhënave personale).

Nëse edhe krahas sugjerimeve, nuk respektohet këshilla juaj nga ana e pronarit të procesit zyrtar, kjo çështje duhet t'i drejtohet pa prolongim udhëheqësisë më të lartë (më hollësisht në pjesën e "Detyrave këshilluese").

Potencojmë se nga Ju pritet që të mbani evidencë të plotë për kontrollet, vlerësimet e realizuara, si dhe këshillat e dhëna.

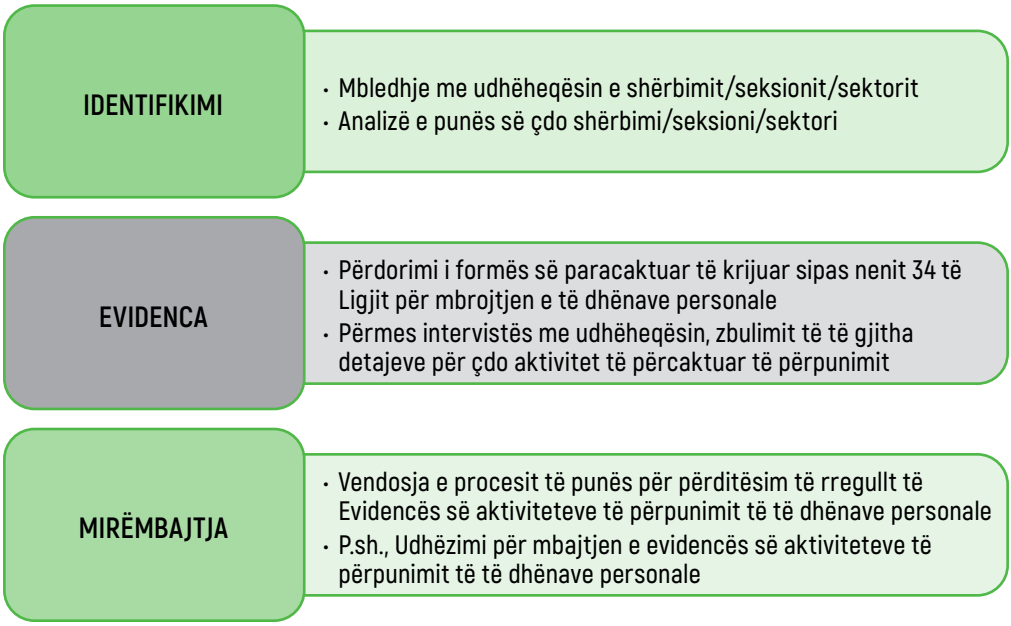


Foto: Fazat e procesit të krijimit të evidencës së aktiviteteve për përpunimin e të dhënave personale

Në vazhdimësi disa shembuj të Evidencës së aktiviteteve të përpunimit:

Shembull	Sistemi për videombikëqyrje
Kontrollori	Ministria/Komuna/Agjencia
Kategoria e subjekteve dhe kategoria e të dhënave personale	Videoincizime nga vizitorët e institucionit
Qëllimi	Mbrojtja e pronësisë, mbrojtja e jetëve dhe shëndetit të të punësuarve për shkak të natyrës së punës që kryhet
Marrësi	Ministria/Komuna/Agjencia
Afati për fshirjen e të dhënave	30 ditë
Masat teknike dhe organizative	Akti i veçantë për mënyrën e kryerjes së videombikëqyrjes
Transferimi i të dhënave personale	/

*Fotografia 2 – Shembulli i Evidencës së aktiviteteve të përpunimit të të dhënave personale.

Me përfundimin e Funksionit dhe detyrës preliminare 1 dhe 2 të Funksionit organizativ duhet të keni përgjigje ndaj pyetjes në vijim:

Hapi 1: Aktivitetet e përcaktuara për përpunimin e të dhënave personale

- lloji i të dhënave personale që përpunohen dhe për cilin qëllim, si dhe kush dhe si përpunohet;
- sistemet që përdoren për përpunim të të dhënave personale.

Hapi 2: Të përcaktuara bazat juridike për përpunimin e të dhënave personale

- mënyrë e përcaktuar ligjore për mbledhjen dhe përpunimin e të dhënave personale;
- të dhënat personale janë evidentuar për qëllim konkret dhe ndiqen udhëzimet për përpunimin e të dhënave personale

Hapi 3: Procese të përcaktuara afariste që imponojnë siguri më të madhe (prioretizimi i tyre!)

- shërbime, sisteme, hapësira dhe të dhëna që duhet të mbrohen, si dhe lidhshmëria e tyre e ndërsjellë

Detyra 3: Vlerësimi i rreziqeve lidhur me aktivitetet e përpunimit të të dhënave personale

Harmonizimi kërkon që të përcaktohen rreziqet relevante, në bazë të regjistrimit të realizuar të aktiviteteve për përpunimin e të dhënave personale dhe krijimin e Evidencës (Regjistrit) të atyre aktiviteteve (Detyra 1), së bashku me pasqyrën e atyre aktiviteteve (Detyra 2).

LMDHP-ja nuk kërkon përfshirje të qartë të oficerit për mbrojtjen e të dhënave personale për realizimin e vlerësimit të përgjithshëm të rreziqeve: përfshirja e tyre parashihet vetëm në aspekt të analizës më të thelluar të rreziqeve, respektivisht realizimit të vlerësimit të ndikimit të mbrojtjes së të dhënave personale, kur identifikohet rrezik i lartë për të drejtat dhe liritë e personave fizikë. Mirëpo, në praktikë rekomandohet që të përfshiheni edhe Ju, në përgjithësi gjatë përgatitjes së vlerësimit të përgjithshëm të rreziqeve të kësaj sfere.

Rreziqet që nevojitet të jenë objekt i vlerësimit nuk i përfshijnë vetëm rreziqet e sigurisë, por edhe probabilitetin dhe ndikimin e cenimit të sigurisë, gjatë aktiviteteve të përpunimit të të dhënave personale që mund të reflektojnë ndaj të drejtave dhe lirive të të dhënave personale, por edhe të individëve tjerë të prekur.

Gjatë përpilimit të vlerësimit lidhur me rreziqet nga aktivitetet e përpunimit të të dhënave personale, merren parasysh natyra, vëllimi, konteksti dhe qëllimet e përpunimit, të cilat janë karakteristike për institucionin Tuaj, respektivisht shfrytëzohet qasje e bazuar në rrezik (nuk zbatohet më parimi i njëjtë për të gjithë, respektivisht qasja universale).

Në pajtim me Rregulloren për sigurinë e përpunimit të të dhënave personale[21] (në tekstin e mëtejmë: Rregullore e sigurisë), gjatë identifikimit dhe vlerësimit të rreziqeve (menaxhimit me rreziqe), kontrollorët i marrin parasysh rreziqet lidhur me përpunimin e të dhënave personale, veçanërisht nga shkatërrimi, humbja, ndryshimi i rastësishëm ose joligjor, zbulimi i paautorizuar ose qasja e paautorizuar në të dhënat që janë transferuar, që ruhen ose përpunohen në ndonjë mënyrë tjetër. Në këtë drejtim, Ju jeni përgjegjës për harmonizimin e nivelit të masave të sigurisë për përpunim në pajtim me Rregulloren e sigurisë, ku me ndihmën dhe këshillimin tuaj pritet që të sigurohet një nivel adekuat i sigurisë për këto përpunime të të dhënave personale që janë pjesë e proceseve zyrtare të institucionit.

Vlerësimi duhet doemos ta përmbajë "së paku" këtë:

I. përshkrimi sistematik i aktiviteteve të parapara për përpunim dhe qëllimet e përpunimit;

II. vlerësimi i domosdoshmërisë dhe proporcionalitetit të aktiviteteve të përpunimit të të dhënave personale në raport me qëllimet;

- ❖ përcaktohen masa të parapara të harmonizimit edhe atë:
  - masa që kontribuojnë për proporcionalitetin dhe domosdoshmërinë e përpunimit të të dhënave personale, në bazë të:
    - » qëllimit(eve) konkrete, eksplicite dhe legjitime;
    - » ligjshmërisë së përpunimit;
    - » adekuates, relevantes dhe të kufizuara ndaj të dhënave të nevojshme;
    - » kohëzgjatje e kufizuar e ruajtjes.
  - masa që kontribuojnë për të drejtat e subjekteve të të dhënave personale:
    - » informata dorëzuar subjektit të të dhënave personale;
    - » të drejtat e subjektit;
    - » raportet me përpunuesit;
    - » masat mbrojtëse rreth transferimit(eve) në vende të treta;
    - » konsultim paraprak me Agjencinë për Mbrojtjen e të Dhënave Personale.

III. vlerësimi i rreziqeve mbi të drejtat dhe liritë e subjekteve të të dhënave personale:

- » vlerësohet prejardhja, natyra, veçantia dhe serioziteti i rreziqeve ose, më konkretisht, për secilin rrezik (qasje të paautorizuar, ndryshim

[21] („Gazeta zyrtare e RMV, nr. 122 nga data 12.5.2020")

i padëshiruar ose humbje e të dhënave), lidhur me subjektet e të dhënave personale;

» merren parasysh burimet e rreziqeve;

» identifikohen ndikimet potenciale mbi të drejtat dhe liritë e subjekteve të të dhënave personale, në rast të ngjarjeve që përfshijnë qasje të paautorizuar, ndryshim ose humbje të padëshiruar të të dhënave;

» identifikohen kërcënimet që mund të sjellin deri te qasja e paautorizuar, ndryshimi ose humbja e padëshiruar e të dhënave;

» vlerësohet edhe probabiliteti dhe serioziteti; dhe

IV. masat e parapara për përballje (mitigim) të rreziqeve, përfshirë edhe masat mbrojtëse, masat dhe mekanizmat e sigurisë për mbrojtjen e të dhënave personale, si dhe dëshmimin e harmonizimit, duke marrë parasysh të drejtat e subjekteve të të dhënave personale dhe personave të tjerë të përshirë.

Në këtë drejtim, vlerësimi i rreziqeve përfshin katër hapa edhe atë:

1. Përcaktimin e aktivitetit për përpunimin e të dhënave personale dhe përmbajtjen e tij;
2. Kuptimin dhe vlerësimin e ndikimit ndaj të drejtave dhe lirive të subjekteve të të dhënave personale;
3. Përcaktimin e kërcënimeve të mundshme dhe vlerësimin e probabilitetit për paraqitjen e kërcënimeve;
4. Vlerësimin e rrezikut (probabilitetin për paraqitjen e kërcënimit dhe ndikimit nëse paraqitet ai).

» Së këndejmi, flasim për katër sfera kryesore për vlerësimin e rreziqeve, edhe atë:

» Resurset teknike dhe të rrjetit (pajisje harduerike dhe softuerike);

» Proceset/procedurat lidhur me aktivitetet e përpunimit të të dhënave personale;

» Palët e ndryshme të përfshira në aktivitetet e përpunimit të të dhënave personale;

» Sektori zyrtar dhe vëllimi i përpunimit.

(në Shtojcën numër 4 të këtij Udhëzuesi, mund të gjeni propozim-qasjen për realizimin e vlerësimit të rreziqeve të propozuar nga Agjencia Evropiane për Rrjetëzim dhe Siguri të Informacioneve, që bazohet në standardin ndërkombëtar ISO 27005[22]: Kërcënime nga keqpërdorimi i vulnerabilitetit të mjeteve që mund

[22] ISO/IEC 27005 "Information technology - Security techniques - Information security risk management"

të shkaktojnë dëm për organizatën (Threats abuse vulnarabilities of assets to generate harm for the organisation", rekomanduar edhe nga Agjencia Italiane për Mbrojtjen e të Dhënave Personale).

Faktorët gjatë vlerësimit të rrezikut

Në përgjithësi kur vlerësohet një rrezik i caktuar, nevojitet që ajo të behët në mënyrë objektive, respektivisht të merren parasysh probabiliteti dhe ndikimi nga paraqitja e këtij rreziku ndaj të drejtave dhe lirive të subjekteve të të dhënave personale.

Vlerësimi i rreziqeve për të drejtat dhe liritë e subjekteve si rezultat i cenimit ka fokus të ndryshëm nga rreziqet që vlerësohen. Vlerësimi i përfshin të dy llojet e rreziqeve: rreziku që përpunimi i të dhënave personale të mos realizohet sipas planifikimit dhe rrezikut në rast të cenimit të sigurisë së të dhënave personale.

Shembull:

Vlerësimi i ndikimit gjatë mbrojtjes së të dhënave personale (në tekstin e mëtejmë: VNMDHP) propozon se përdorimi i një produkti të caktuar softuerik të sigurisë për mbrojtjen e të dhënave personale është masë adekuate për të siguruar nivelin e sigurisë që është adekuat me rrezikun që ndryshe do ta shkaktonte përpunimi i të dhënave personale, për subjektet e të dhënave personale. Megjithatë, nëse cenimi paraqitet më vonë, respektivisht për atë do të vetëdijesohen në mënyrë plotësuese, ajo do ta ndryshojë përshtatshmërinë e nivelit të sigurisë së softuerit dhe për këto arsye ai duhet të jetë objekt i vlerësimit të serishëm si pjesë e VNMDHP-së aktuale).

Në fakt, më vonë shfrytëzohet vulnerabiliteti i mjetit dhe vjen deri te cenimi i sigurisë. Kontrollori duhet t'i vlerësojë rrethanat specifike të cenimit, se cilat të dhëna personale janë të prekura dhe ka ndikim potencial ndaj individëve, si dhe sa ka probabilitet që ky rrezik të materializohet (p.sh natyra, ndjesia dhe vëllimi i të dhënave, mundësia për identifikimin e subjekteve të të dhënave personale, pasojat, mundësia për t'i kthyer të dhënat e humbura, dëmi i shkaktuar, etj.)

Si praktikë e mirë gjatë vlerësimit rekomandohet që të merren parasysh kriteret në vijim:

1. Lloji i cenimit i cili mund të ndikojë mbi nivelin e rrezikut

Shembull:

Cenimi i konfidencialitetit mund të jetë në aspekt të zbulimit të të dhënave mjekësore nga persona të paautorizuar të cilët mund të shkaktojnë pasoja të ndryshme ndaj individit, respektivisht të dhënat të humben dhe të mos jenë më të disponueshme.

2. Natyra, ndjeshmëria dhe vëllimi i të të dhënave personale

Kategoria e të dhënave personale, siguria e të cilave është cenuar, paraqet faktor kryesor gjatë vlerësimit të rreziqeve. Sa më të ndjeshme të dhënat, aq më i madh është rreziku nga dëmi ndaj subjekteve të prekur të të dhënave personale, nëse ato në njëfarë mënyre veç më janë publikisht të qasshme.

Për shembull, zbulimi i emrit dhe adresës së ndonjë subjekti me gjasë nuk do të shkaktojë dëm të konsiderueshëm. Mirëpo, nëse prindit biologjik i zbulohen emri dhe adresa e adoptuesit, pasojat e privatësisë mund të kenë ndikim të konsiderueshëm edhe për adoptuesin dhe për fëmijën.

Prishjet që përfshijnë të dhëna shëndetësore, dokumente identifikuese ose të dhëna financiare siç është kredia, detajet e kartelës pagesore, etj, vetvetiu nuk shkaktojnë dëm, por nëse shfrytëzohen në kombinim me të dhëna të tjera, të njëjtat mund të shfrytëzohen për vjedhjen e identitetit të subjektit të të dhënave personale.

3. Thjeshtësia gjatë identifikimit të individëve

Faktor i cili gjithashtu duhet të vlerësohet është nëse pala që ka qasje në të dhënat e kompromentuara personale, ka mundësi që të identifikojë individë të caktuar.

Varësisht nga rrethanat, identifikimi mund të bëhet përmes shfrytëzimit të drejtpërdrejtë të të dhënave të cenuara personale, ose do të nevojiten aktivitete plotësuese për të zbuluar identitetin e individit.

Në këtë drejtim, zbatimi i masave të caktuara teknike, si p.sh pseudonimizimit, do të mundësojë përpunimin e të dhënave personale, në mënyrë që aktiviteti i përpunimit nuk mund të shpjerë deri te një subjekt i caktuar i të dhënave personale, pa u nevojitur informata shtesë për atë person. Megjithatë, kjo do ta zvogëlojë edhe probabilitetin për paraqitjen edhe të individëve të tjerë, që mund të identifikohen, në rast të cenimit të sigurisë. Vlerësimi i secilit aktivitet të përpunimit është individual, duke marrë parasysh se teknikat e pseudonimizimit, vetvetiu nuk mund të konsiderohen se i bëjnë të dhënat në tërësi të pakuptueshme, si dhe se të dhënat e pseudonimizuara ende konsiderohen si të dhëna personale.

4. Serioziteti i pasojave për subjektet e të dhënave personale

Nëse cenimi ka të bëjë me të dhënat personale për kategoritë e cenueshme të subjekteve, ai do të shkaktojë dëm edhe më të madh.

Nëse të dhënat personale janë në duart e personave qëllimet e të cilëve janë të panjohura ose eventualisht qëllimkeqe, ai ndikon mbi nivelin e rrezikut potencial. Në këtë mënyrë vihet në pikëpyetje konfidencialiteti, për arsye se të dhënat personale i janë zbuluar personit të tretë, ose marrë tjetër edhe atë si rezultat i gabimit.

Për shembull, kur të dhënat personale dërgohen rastësisht në një seksion të gabuar të organizatës ose në një organizatë të jashtme të shfrytëzuar më shpesh

– furnizues. Ndërkaq, kontrollori mund të kërkojë nga marrësi ose t'i kthejë ose t'i shkatërrojë në mënyrë të sigurt të dhënat e marra. Në të dy rastet, nevojitet që kontrollori të jetë në kontakt të vazhdueshëm me palët e tretë, që të jetë i vetëdijshëm për procedurat e tyre, historinë si dhe detajet e tjera për marrësin. Nëse marrësi është konfidencial, kjo mund të çojë deri te ulja ose shmangja e tërësishme e pasojave cenimi, por ajo nuk nënkupton se nuk do të vijë deri te cenimi. Por, sërish kjo është objekt i vlerësimit individual.

Megjithatë, kontrollori ende duhet t'i ruajë informatat lidhur me cenimin si pjesë e detyrës së përgjithshme për mbajtjen e evidencës për cenimet.

Duhet të merret parasysh edhe kohëzgjatja e pasojave për individët, veçanërisht nëse ndikimi është i konsiderueshëm, ndërsa efektet janë afatgjate.

5. Karakteristikat e veçanta të subjekteve të të dhënave personale

Cenimet mund të ndikojnë ndaj të dhënave personale për një kategori të caktuar të subjekteve, p.sh. fëmijë ose subjekte tjera të cenueshme, që mund të ekspozohen edhe ndaj rreziqeve edhe më të mëdha. Edhe faktorë të tjerë për subjektin mund të ndikojnë mbi vetë cenimin.

6. Karakteristikat e veçanta të kontrollorit të të dhënave personale

Natyra dhe roli i kontrollorit dhe aktivitetet e tij mund të ndikojë mbi nivelin e rrezikut për individë si rezultat i cenimit konkret të sigurisë së të dhënave personale. Për shembull, institucioni mjekësor që përpunon kategori të posaçme të dhënave personale, paraqet kërcënim më të madh për subjektet, në rast se shkaktohet cenim i të dhënave të tyre personale.

7. Numri i personave të prekur

Në përgjithësi, sa më i madh numri i personave të prekur, aq më i madh është ndikimi i prishjes. Megjithatë, vetë cenimi mund të ketë ndikim serioz madje edhe ndaj një personi, varësisht nga natyra e të dhënave personale dhe kontekstit në të cilin të dhënat janë të kompromentuar. Prandaj, me rëndësi të veçantë është të shqyrtohet probabiliteti dhe serioziteti i ndikimit të palëve të interesuara.

Në bazë të vlerësimit të realizuar dhe rreziqeve të përcaktuara, prej Jush pritet që t'i jepet prioritet dhe të fokusoheni në çështjet që paraqesin rrezik të lartë ndaj të drejtave dhe lirive të subjekteve, të dhënat personale e të cilëve përpunohen nga ana e Institucionit tuaj.

Për përpunimin që paraqet rrezik të lartë për të drejtat dhe liritë e personave fizik, nevojitet që ta njoftoni personin përgjegjës ose personat e obliguar për menaxhim me rreziqet (nëse ka të përcaktuar) dhe të propozoni masa për zbutjen ose veprimet alternative. Nëse këshilla juaj nuk ndiqet, nevojitet që atë t'ia drejtoni udhëheqësisë më të lartë.

Për të gjitha këto aktivitete, mbani evidencë të plotë dhe ruani shënime.

Këto shënime "do të tregojnë se përpunimi është realizuar në pajtim me rregullativën për mbrojtjen e të dhënave personale" – respektivisht se ato rreziqe me të vërtetë janë vlerësuar dhe se masat e ndërmarra janë adekuate me menaxhimin e tyre, në drejtim të "detyrës për të demonstruar harmonizim" me LMDHP-në.

Gjithashtu, prej Jush pritet që të konstatoni se cilat sfera janë lëndë e revizionit/kontrollit/hetimit të brendshëm ose të jashtëm, çfarë trajnimi/edukimi/ushtrimi duhet të organizohen për të punësuarit dhe se cilave aktivitete të përpunimit të të dhënave personale në kuadër të proceseve zyrtare duhet që të punësuarit t'u kushtojnë vëmendje të posaçme.

SHEMBUJ:

- Të dhënat personale të mbledhura për një qëllim (përpunimi i kartelës për qasje) shfrytëzohen edhe për qëllime të tjera (publikimi i fotografisë në rrjetet sociale), respektivisht qëllimet për të cilat nuk ka bazë adekuate juridike dhe/ose subjektet e të dhënave personale nuk janë të informuar për përpunimin e planifikuar sekondar, që do të ishte edhe më serioze në rast se ekziston zbulim i të dhënave për palët e treta;

Sqarim: Kjo mund të rezultojë edhe me atë që subjektet e të dhënave personale të mos jenë të informuar (ose të mos pajtohen) për përpunimin sekondar, që nga ana tjetër do të kishte pasoja negative ndaj tyre (p.sh, në vendin e punës ose te aplikimet për marrjen e ndihmës sociale ose financiare, etj.). Gjithashtu, me gjasë është se të dhënat personale të marra për një qëllim janë të sakta mjaftueshëm, respektivisht relevante për përdorimin në një kontekst krejtësisht të ndryshëm.

- Ruajtja dhe/shfrytëzimi i të dhënave personale (pasi më nuk janë të nevojshme për qëllimin që janë mbledhur) me formë të pseudonimizuar ose anonimizuar (për përdorim të mëtejshëm për një qëllim të ri dytësor).

Sqarim: Duke marrë parasysh rrezikun nga riidentifikimi i gjoja të dhënave tërësisht të anonimizuara, në secilën ruajtje ose përdorim të këtyre të dhënave, nevojitet që të shihet se paraqet rrezik për të drejtat dhe liritë e subjekteve të të dhënave personale (që mund të shpjerë në "rrezik të lartë", që kërkon përgatitje të vlerësimit të ndikimit ndaj mbrojtjes së të dhënave personale). Në këtë drejtim, duhet t'i kontrolloni rreziqet nga aspekti i mundësisë për riidentifikimin të personit për cilindo përdorim specifik dhe të parashihni masa të përforcuara për zbutjen e tyre, e deri te ndalimi për përpunimin e tyre të mëtutjeshëm.

- Shfrytëzimi i të dhënave jorelevante, të pasakta ose të vjetëruara

Sqarim: Pasoja të mundshme të ngjashme negative siç edhe u sqaruan në shembullin paraprak

- Moskushtimi i vëmendjes së nevojshme në aspekt të "interesave ose të drejtave dhe lirive themelore të subjektit të të dhënave personale që kërkojnë mbrojtjen e të dhënave personale, veçanërisht kur subjekti i të dhënave personale është fëmijë".

- Informimi joadekuat i subjekteve i të dhënave personale për të gjitha detajet për të cilat patjetër duhet të informohen me ç'rast subjektet nuk do të kenë informatë rreth asaj se për cilat qëllime përpunohen të dhënat e tyre personale, sa kohë do të ruhen ato të dhëna personale, a do të transferohen tek persona të tretë, etj.

Sqarim: Kjo mund të rezultojë edhe me atë që subjektet e të dhënave personale të mos mund që në tërësi t'i realizojnë të drejtat e tyre, respektivisht interesat ose të drejtat dhe liritë themelore të subjektit të të dhënave personale të cilat duhet të mbrohen.

- Transferimi i të dhënave personale në një vend të tretë ku nuk është siguruar "nivel adekuat" i mbrojtjes së të dhënave personale, nuk janë zbatuar masa adekuate mbrojtëse ose një set i rregullave të detyrueshme korporative, respektivisht nuk bën pjesë në një prej shmangieve të theksuara për situatat e caktuara, të përkufizuara në LMDHP-në. Kjo përfshin shfrytëzimin e "shërbimeve në re" (cloud computing) që shfrytëzon server (ose serverë) të cilët janë të vendosura në vende të treta.

Sqarim: Keni parasysh se "shërbimet në re" (cloud computing) në vete bartin rreziqe specifike që duhet të trajtohen me vëmendje nga ana e kontrollorëve. Për arsye se, në mënyrë inherente sjellin rreziqe të mëdha, nëse shfrytëzohen llojet e këtyre të shërbimeve, nevojitet që për to të përgatitet Vlerësim adekuat i ndikimit mbi mbrojtjen e të dhënave personale.

Pas mbarimit të kësaj detyre, duhet të keni mundësi të përgjigjeni në fjalitë në vijim:

Hapi 4: I keni analizuar rreziqet potenciale, përkatësisht:

4.1. Janë identifikuar rreziqet: (është përcaktuar nëse siguria e të dhënave personale u nënshtrohet rreziqeve siç janë katastrofat natyrore, përgjegjësitë e përcaktuara në mënyrë të pamjaftueshme në kuadër të organizatës, ose problemeve teknike potenciale etj);

4.2. Janë vlerësuar pasojat e mundshme:
- serioziteti i pasojave në rast të incidentit
- skenarë të përcaktuara dhe nëse ato ndikojnë mbi të dhënat që duhet të mbrohen në mënyrë të veçantë (të dhënat për shëndetin ose detajet nga dosja e personave të punësuar etj.)

4.3. Është vlerësuar probabiliteti:
- të ndodhë ndonjë incident
- përvoja e institucionit i cili mund ta lehtësoje vlerësimin e seriozitetit të dëmit nga paraqitja a ngjarjes së tillë
- informata të nevojshme që të konstatohet dëmi i mundshëm.

4.4. Është përcaktuar shkalla e rrezikut:
- rreziqet që nënkuptojnë shkallë të lartë të ndikimit dhe shkallë të lartë të probabilitetit
- rreziqet që do të shkaktojnë dëm më të vogël dhe ekziston probabilitet më i vogël për t'u paraqitur.

Në pajtim me Rregulloren për sigurinë e përpunimit të të dhënave personale, në aspekt të zbatimit të masave teknike dhe organizative, japim udhëzime dhe drejtime të caktuara sipas të cilave mund të udhëhiqeni dhe të veproni në punën tuaj (Shtojca 7 e këtij Udhëzuesi).

Detyra 4: Menaxhimi me aktivitetet e përpunimit të të dhënave personale për të cilat ka gjasë se do të rezultojnë me "rrezik të lartë", pas lirive dhe të drejtave të subjekteve, në bazë të vlerësimit të realizuar të ndikimit mbi mbrojtjen e të dhënave personale.

Vlerësimi i përgjithshëm i rreziqeve, të përshkruar në Detyrën 3 realizohet edhe për aktivitetet e përpunimit të të dhënave personale që paraqesin "rrezik të lartë për të drejtat dhe liritë e personave fizikë".

LMDHP-ja thekson qartë se kjo në veçanti është rasti kur zbatohen teknologjitë e reja. Për këto arsye, nevojitet që Kontrollori të bëjë vlerësimin e ndikimit ndaj mbrojtjes së të dhënave personale, para se të vazhdojë me përpunimin e mëtejmë të të dhënave personale.

Agjencia për Mbrojtjen e të Dhënave Personale ka miratuar, në formë të akteve nënligjore – Rregulloren për procesin e vlerësimit të ndikimit ndaj mbrojtjes së të dhënave personale[23], Listën e llojeve të aktiviteteve të përpunimit për të cilat kërkohet vlerësimi i ndikimit ndaj mbrojtjes së të dhënave personale[24], si dhe Listën e llojeve të aktiviteteve të përpunimit për të cilat nuk kërkohet vlerësimi i ndikimit ndaj mbrojtjes së të dhënave personale[25].

Përgatitja dhe vlerësimi i ndikimit ndaj mbrojtjes së të dhënave personale (në tekstin e mëtejmë: VNMDHP) paraqet një mjet të dobishëm për menaxhim me rreziqet ndaj të drejtave dhe lirive të subjekteve të të dhënave personale, ndërsa menaxhimi me rreziqet në sfera të ndryshme (p.sh. siguria informatike) është fokusuar para se gjithash në rreziqet ndaj sigurisë informatike me të cilat ballafaqohet organizata.

Qëllimet e VNMDHP-së janë identifikimi dhe vlerësimi i rreziqeve të mëdha mbi të drejtat dhe liritë e personave fizikë, të përfshirë në aktivitetet e përpunimit, gjatë shfrytëzimit të teknologjive të reja, duke marrë parasysh natyrën, vëllimin, kontekstin dhe qëllimet e përpunimit, burimet e rrezikut, si dhe masat që mund të ndërmerren për të zbutur këto rreziqe, në mënyrë adekuate në aspekt të teknologjisë së disponueshme dhe shpenzimeve për implementim. Njëherë, duhet të evidentohen konstatimet, vlerësimi dhe masat e ndërmarra (ose të pandërmarra, duke theksuar arsyet për të njëjtën), në mënyrë që të mund të "tregohet harmonizimi" me kërkesat e LMDHP-së, në pajtim me parimin e "llogaridhënies" në aspekt të përpunimit të vlerësuar.

[23] („Gazeta zyrtare e RMV-së, nr. 122 nga data 12.5.2020")
[24] („Gazeta zyrtare e RMV-së, nr. 122 nga data 12.5.2020")
[25] („Gazeta zyrtare e RMV-së, nr. 122 nga data 12.5.2020")

Neni 39, paragrafi 3 i LMDHP-së përcakton se "rreziqet e mëdha" për të drejtat dhe liritë e personave fizikë, mund të dalin në veçanti nga:

- përpunimi i automatizuar, përfshirë edhe profilizimin, në bazë të të cilit sillen vendime që prodhojnë veprim juridik, respektivisht dukshëm ndikojnë ndaj personit fizik;
- përpunimi i vëllimit të madh të kategorive të posaçme të të dhënave personale ose të dhënave personale që kanë të bëjnë me aktgjykime ndëshkimore dhe vepra penale nga neni 14 të LMDHP-së; ose
- mbikëqyrja sistematike e hapësirave të disponueshme publikisht në përmasa më të mëdha.

Përpunimi automatik, përfshirë edhe profilizimin:

Vendimmarrja e automatizuar, bazuar në profilizimin, mund të çojë në vendime jo të drejta (sepse nuk ekziston person i cili është identik me një individ tjetër dhe se asnjë sistem nuk i posedon të gjitha të dhënat për një person) ose vendime jodemokratike, të cilat mund të përfshijnë edhe rezultat diskriminues; përdorimi i një kategorie të posaçme të të dhënave personale, gjithashtu mund të çojë në diskriminim (pa marrë parasysh se a është e qëllimshme ose jo); përdorimi i të dhënave të parëndësishme personale për shitje, mund të zbulojë probleme intime shëndetësore ose shtatzëni; dhe ndjekja sistematike e njerëzve në vende publike që mund të ketë efekt të tmerrshëm mbi realizimin të të drejtave themelore siç janë e drejta e lirisë së shprehjes, grumbullimit, protestës, etj.

Rreziqet mund të kombinohen dhe ta forcojnë në mënyrë të ndërsjellë veprimin e tyre, si për shembull gjatë përdorimit të teknologjisë për njohje të personave për ndjekje në vende publike nga ana e policisë, me qëllim të "identifikimit" dhe parashikimit të sjelljes së keqe.

Ndërkaq, në mënyrë që këto rreziqe të materializohen, nuk nevojitet cenimi i të dhënave personale: rreziqet dalin nga rreziku inherent (rreziku i trashëguar) i vetë aktiviteteve të përpunimit të të dhënave personale, madje edhe nëse përpunimi bëhet në pajtim me specifikat e tyre pa u cenuar siguria.

Më tepër shembuj mund të gjeni në Shtojcën nr. 4 të këtij Udhëzimi.

Shfrytëzimi i shërbimeve nga persona të jashtëm

Gjatë vlerësimit të rreziqeve, nëse përpunimi i të dhënave personale për nevojat e organeve të administratës shtetërore, përfshinë kategori të posaçme të të dhënave personale në kuptimin tekniko-juridik të Ligjit ("kategori të posaçme të të dhënave"), ose të ndjeshme në terme më të përgjithshme, siç janë të dhënat financiare ose të dhënat për regjistrim, ajo mund të realizohet në bashkëpunim me personat e jashtëm.

Në aspekt të realizimit të kontrollit të detajuar të personave të jashtëm (palë të treta, përpunues, ofrues të jashtëm të shërbimeve, furnizues, etj.), nevojitet që para hyrjes në raport kontraktues, për secilin person të jashtëm të bëhet:

- kontroll nëse është harmonizuar me dispozitat ligjore për mbrojtjen e të dhënave personale;
- kontroll nëse ka qenë nën hetim për cenim të sigurisë së të dhënave personale;
- identifikimin e klientëve të tij të tjerë;
- referencat negative ose publikimet e përgjithshme negative që mund të ndikojnë në reputacionin e tij;
- kontroll nëse është i certifikuar sipas ISO27001, PCI DSS ose ndonjë standardi tjetër nga sfera e sigurisë informatike (sidomos për përpunuesin);
- rishikimi i dokumentacionit për sigurinë dhe mbrojtjen e të dhënave personale;
- realizimi i vizitave dhe kontrolleve në terren (kjo parashihet me planin për kontrolle të drejtpërdrejta ose të tërthorta operative, në përputhje me rezultatet nga vlerësimi i realizuar i rreziqeve dhe prioritizimin e tyre);
- identifikimi i selisë;
- analizë e shkurtë nga njoftimi me zinxhirin e furnizimeve dhe nënkontraktuesit e tyre.

Vidembikëqyrja dhe analiza e rrezikut:

Administrata shtetërorë e suedeze për mbrojtjen e të dhënave personale e dënoi komunën Skeleftea me 200.000 SEK (17.000 euro) për shkak të shkeljes së GDPR-së. Vlerësimi i agjencisë shtetërore është se gjimnazi në Skeleftea derisa ka realizuar një pilot test të sistemit për identifikimin e personave i ka shkelur të dhënat personale të 22 nxënësve. Megjithëse ideja kishte qenë që sistemi të shfrytëzohet për ndjekje më të lehtë të pranisë së nxënësve, GDPR-ja i klasifikon ato të dhëna si një kategori të posaçme të të dhënave personale, me kufizimet e posaçme të përdorimit të tyre.

Me rritjen e ndjekjes së personave përmes videombikëqyrjes zvogëlohet liria e lëvizjes dhe sjellja e personave dhe privatësia e tyre, veçanërisht atij që realizohet në vendet e punës.

Gjatë vlerësimit të rreziqeve udhëhiquni nga përmbushja e këtyre obligimeve, lidhur me videombikëqyrjen:

- argument i qartë që është përgjegjës për videombikëqyrjen, përmes sigurimit të njoftimit që i përmban këto elemente të detyrueshme: derisa bëhet videombikëqyrje, emri/titulli i kontrollorit që e kryen videombikëqyrjen si dhe mënyra në të cilën mund të marrin informata për atë se ku dhe sa kohë ruhen

incizimet nga sistemi i videombikëqyrjes.

- respektimi i rregullave për atë se cilat të dhëna dhe në çfarë mase mund të mblidhen dhe ruhen (përfshirë edhe qëllimin e instalimit të videombikëqyrjes, afatin e ruajtjes së materialeve të incizuara, etj.);
- bazë e kufizuar juridike (mbrojtja e jetës ose shëndeti i njerëzve, mbrojtja e pronësisë, mbrojtja e jetës dhe shëndetit të punonjësve për shkak të natyrës së punës ose sigurimit të kontrollit të hyrje-daljes nga hapësirat zyrtare ose të punës vetëm për qëllime të sigurisë).
- zbatimi i masave teknike dhe organizative (instalimi i kamerës për përmbushjen e qëllimeve të videombikëqyrjes, autorizim për shikimin e incizimeve, evidenca e qasjes së autorizuar/paautorizuar, mbrojtja e emrit dhe fjalëkalimit të përdoruesit, etj.)
- afati i ruajtjes (maksimalisht 30 ditë, përveç nëse nuk është paraparë ndonjë afat më i gjatë me ndonjë ligj tjetër),
- ndalim për incizim në hapësira të caktuara (mbikëqyrje në gardëroba, zhveshtore, nyje sanitare dhe hapësira të tjera të ngjashme.)
- akt i brendshëm – Rregullore për mënyrën e realizimit të videombikëqyrjes, me të cilin do të rregullohen, p.sh., autorizimi i qasjes në incizimet, sistemi i automatizuar i incizimeve (logeve), transparenca), sistem i mbrojtur me fjalëkalim, trajnimi i punonjësve, etj.
- Deklaratë/Njoftim i miratuar dhe i publikuar për privatësi.

Shembuj:

Videombikëqyrja e vendit të punës dhe ambientit publik

Shumë herë kur shkoni në mbledhje, do të shihni se zyra dhe ambiente të caktuara janë nën videombikëqyrje, qëllimi i së cilës duhet të jetë mbrojtja e njerëzve, pronës dhe biznesit. Shpeshherë, kompanitë pa vlerësim të rrezikut, me iniciativë të tyre instalojnë sistem për videombikëqyrje, me të cilën bëhet shkelja në domenin e mbrojtjes së të dhënave personale. Duhet të theksohet se videombikëyrja e tillë është i papërdorshëm thellësish sepse videomateriali i saj mund të kontestohet lehtë në çdo procedurë dhe në thelb përbën rrezik të madh për institucionin i cili e përdor për incizim të punonjëse, vizitorëve dhe personave të tretë në kundërshtim me dispozitat ligjore, përkatësisht i ruan dhe i arkivon të dhënat e tyre personale.

Përgjigja e cila shpesh dëgjohet për pyetjen pse incizohen zyrat ose ambientet tjera publike, është se "ashtu kanë thënë eprorët".

Punëdhënësi duhet ta respektojë privatësinë e të gjithë punonjësve përderisa janë në vendin e punës, përkatësisht parimin e proporcionalitetit, lidhur me qëllimin për të cilin instalohet videombikëqyrja. Teknologjia e re dhe videombikëqyrja e

vazhdueshme, mund të ndikojnë negativisht mbi shëndetin dhe gjendjen fizike të punonjësve dhe mbi aftësinë e punës.

Në përputhje me të lartpërmendurën, në aspekt të përfshirjes së palëve të interesuara në përgatitjen e vlerësimit të rreziqeve, këshilla Juaj është me rëndësi kryesore.

Prandaj, kontrollori në bashkëpunim me Ju, do të bëjë vlerësim të përshtatur ndaj nevojave të institucionit, e duke u bazuar në përvojën ndërkombëtare për vlerësim të rrezikut, për shembull., në përputhje me standardin ISO 31000 Risk Management.

Qëllimi kryesor i incizimit nga vlerësimi i realizuar është të ketë dëshmi se është bërë VNMDHP adekuate, e thellë, në përputhje me LMDHP-në, përmes përmbushjes së kritereve të lartpërmendura.

Sqarim më të thellë të faktorëve që tregojnë se ka gjasa të rezultojnë me "rrezik të lartë" dhe për të cilat nevojitet detyrimisht përgatitja e VNMDHP, mund të gjeni në Shtojcën nr. 4 të këtij Udhëzuesi.

Shënim:

Dorëzimi i njoftimit në Agjencinë për Mbrojtje të të Dhënave Personale:

- nevojitet të evidentohet në mënyrë elektronike në Evidencën për përmbledhje të të dhënave personale me rrezik të lartë, me emrin e përdoruesit dhe fjalëkalimin për qasje në sistemin;
- me përjashtim, për ato që tashmë janë regjistruar në Regjistrin Qendror të Përmbledhjeve të të dhënave personale, nevojitet që të dorëzohet Njoftim në formë elektronike përmes faqes së internetit të AMDHP-së për evidentimin e tij.

Forma dhe përmbajtja e formularit të njoftimit është përcaktuar në dispozitat e Rregullores për njoftim për përpunimin e të dhënave personale me rrezik të lartë.

Pas përfundimit të kësaj detyre, duhet të mund t'u përgjigjeni pyetjeve në vijim:

Hapi 5: I keni zgjedhur masat adekuate teknike dhe organizative

- Masat teknike dhe organizative janë zgjedhur në bazë të rreziqeve që duhet të kenë prioritet në zgjidhjen për shkak të shkallës së lartë të seriozitetit dhe probabilitetit
- Duke u udhëhequr në përputhje me arritjet më të larta teknologjike, masat që duhet të shqyrtohen për minimizimin e këtyre rreziqeve
- Masat që mund të zbatohen në vëllim racional (paraqesin shpenzim racional, për shembull prokurimi i makinës për shkatërrimin e dokumenteve të letrës, shrederit (masë teknike) dhe zbatimi i disa udhëzimeve adekuate të punës për shkatërrim të dokumenteve të letrës (masë organizative).

Hapi 6: E keni vlerësuar rrezikun e mbetur

- Rreziqet e përcaktuara të cilat nuk mund të shmangen plotësisht duke aplikuar masa teknike dhe organizative
- Shkalla e seriozitetit dhe probabilitetit të rreziqeve të mbetura

Hapi 7: I keni konsoliduar masat

- Është bërë kombinim i duhur i masave
- Masat janë të përshtatshme për rrethanat e veçanta në organizatën Tuaj

Hapi 8: I keni zbatuar masat e përzgjedhura

- Përcaktimi i (ose përzgjedhjs e) masave që do të zbatohen së pari (në përputhje me nivelin e masave – standard ose i lartë)
- Është përcaktuar pala përgjegjëse për zbatimin e tyre
- Masat e zbatuara që kanë çuar në rezultatin e dëshiruar si rezultat i vlerësimit të realizuar të rrezikut.

Detyra 5: Menaxhimi me cenimin e sigurisë së të dhënave personale;

Ideja për njoftim për cenimin e sigurisë së të dhënave personale nuk është risi në vetvete. Obligimi për njoftim tashmë ishte përfshirë në Direktivën për e-privatësi.[26] Megjithatë, kjo detyrë ishte e kufizuar për ofruesit e komunikimeve elektronike, rrjeteve dhe shërbimeve elektronike. GDPR përdor përkufizimin e njëjtë të "shkeljes së të dhënave personale" siç është ajo e përfshirë në Direktivën për e-privatësi, por pa kufizimin që ka të bëjë me cenimin e sigurisë që çon në shkatërrim e rastësishëm ose të paligjshëm, humbje, ndryshim, zbulim ose qasje të paautorizuar në të dhënat personale të transferuara, të ruajtura ose të përpunuara ndryshe.

Nëse bëjmë një paralele, obligimi për të njoftuar Agjencinë për Mbrojtjen e të Dhënave Personale në rast të shkeljes së të dhënave personale u parashikua edhe me Ligjin e vjetër për mbrojtjen e të dhënave personale (i cili nuk është në fuqi).

[26] Directive 2002/58/EC of the European Parliament and of the Council.

Rregullorja aktuale për mbrojtjen e të dhënave personale parashikon:

- njoftimin e përgjithshëm të organit mbikëqyrës përkatës për çdo cenim të sigurisë së të dhënave personale që mund të rezultojë me rrezik për të drejtat dhe liritë e individëve; dhe
- detyrim për informim të subjekteve të të dhënave për shkeljet e tilla, në rastet kur ka gjasa të rezultojë me „rrezik të lartë“ për të drejtat dhe liritë e personave fizikë..

Ndërkaq, hasim lloje të ndryshme të shkeljeve të të dhënave personale ("cenimi i konfidencialitetit"; "cenimi i integritetit"; "cenimi i disponueshmërisë").

Shembull për cenimin e sigurisë së të dhënave personale është situata në të cilën humbet ose vidhet një pajisje që përmban kopje të bazës së të dhënave për klientë të kontrollorit.

Situatë shtesë e cenimit mund të jetë ajo ku kopja e vetme e bazës së të dhënave është e enkriptuar nga softuer qëllimkeq që bllokon të dhënat e kontrollorit derisa të paguhet shpërblesa, ose është i enkriptuar nga kontrollori me ndihmën e një çelësi që nuk është më në pronësi të tij.

Shembujt e humbjes së disponueshmërisë përfshijnë edhe situata ku të dhënat fshihen rastësisht nga një person i paautorizuar. Nëse kontrollori nuk mund të rivendosë qasjen në të dhëna, për shembull, nga një kopje rezervë, atëherë kjo konsiderohet humbje e përhershme e disponueshmërisë së tyre.

Humbja e disponueshmërisë mund të ndodhë gjithashtu nëse vjen deri te çrregullimi i konsiderueshëm i funksionimit normal të një organizate, për shembull, ndërprerja e energjisë ose sulm i a.q. (denial service), gjë që i bën të dhënat personale të padisponueshme.

Edhe humbja e përkohshme e disponueshmërisë mund të jetë shkelje e të dhënave personale.

Në vazhdim janë disa shembuj të tjerë:

Në spitale, nëse nuk janë të disponueshme të dhëna për gjendjen shëndetësore të pacientëve, qoftë edhe përkohësisht, mund të përbëjë rrezik për të drejtat dhe liritë e personave fizikë; për shembull, operacionet mund të anulohen dhe jetët të vihen në rrezik.

Në të kundërtën, në rast se sistemet e një kompanie mediatike nuk janë të disponueshme për disa orë (p.sh. për shkak të ndërprerjes së energjisë elektrike), nëse me këtë ajo pengohet t'u dërgojë buletine abonentëve të saj, kjo me gjasë nuk do të përbëjë rrezik për të drejtat dhe liritë e personave fizikë.

Sulmi me shpërblesë mund të çojë në një humbje të përkohshme të disponueshmërisë nëse të dhënat mund të kthehen nga një kopje rezervë.

Megjithatë, nëse ndodh një hyrje (ndërhyrje) e paautorizuar në rrjet, njoftimi mund të kërkohet nëse incidenti cilësohet si shkelje e konfidencialitetit (përkatësisht sulmuesi ka qasje të paautorizuar në të dhënat personale), kjo padyshim përbën rrezik për të drejtat dhe liritë e personave fizikë.

LMDHP-ja parashikon që AMDHP-ja duhet të njoftohet jo më vonë se **72 orë** pasi kontrollori është vënë në dijeni për cenimin e sigurisë së të dhënave personale. Përjashtim nga kjo është nëse nuk ka gjasa që cenimi i sigurisë së të dhënave personale të krijojë rrezik për të drejtat dhe liritë e personave fizikë.

Nëse kontrollori vonohet me dërgimin e njoftimit në AMDHP është e nevojshme të dorëzojë arsyetim për shkaqet e vonesës.

Nëse bëhet fjalë për përpunues, ai është i detyruar ta njoftojë kontrollorin menjëherë pasi të mësojë për cenimin e sigurisë së të dhënave personale.

LMDHP-ja gjithashtu përcakton se:

Kontrollori i dokumenton të gjitha cenimet e të dhënave personale, duke përfshirë faktet lidhur me cenimin e të dhënave personale, efektet e tij dhe masat e ndërmarrë për përballje me cenimin. Ky dokumentacion do t'i mundësojë organit mbikëqyrës ta vërtetojë harmonizimin me këtë obligim.

Kini parasysh se kërkesa e fundit ka të bëjë me të gjitha cenimet e sigurisë së të dhënave personale: nuk kufizohet vetëm në cenimet për të cilat duhet të njoftohet Agjencia për Mbrojtjen e të Dhënave Personale, përkatësisht shënimi doemos duhet të përfshijë se për çfarë cenimi të të dhënave personale bëhet fjalë dhe (sipas mendimit të kontrollorit po) "nuk është e sigurt se do të rezultojë me rrezik për të drejtat dhe liritë e personave fizikë".

Shënim: Në Shtojcën nr. 5 janë dhënë 5 shembuj dhe sqarime shtesë lidhur me cenimin e sigurisë së të dhënave personale.

Për sa u përket subjekteve të të dhënave personale, LMDHP-ja përcakton se subjektet duhet të njoftojnë "pa prolongim të panevojshëm", që do të thotë sa më shpejt të jetë e mundur.

Qëllimi kryesor i njoftimit për subjektet është të jepen informata konkrete për hapat që duhet t'i ndërmarrin për t'u mbrojtur. Siç është cekur më lart, varësisht nga natyra e shkeljes dhe rrezikut që e bart, komunikimi në kohë do t'u ndihmojë subjekteve që të ndërmarrin hapa për t'u mbrojtur nga çdo pasojë negative që mund të ndodhë nga cenimi. Në këtë drejtim, LMDHP-ja parasheh elemente të detyrueshme të njoftimit, si dhe përjashtime nga obligimi për nivelin e njoftimit.

Shembull:

Sigurisht keni hasur në situatë që të mësoni qëllimisht ose pa qëllim pse kolegu i punës është në pushim mjekësor. Ana Petrovska ka hapur pushim mjekësor me shifrën e sëmundjes X dhe informatat nga Sektori për resurse njerëzore, përcillen,

ashtu që punonjësit tjerë njoftohen me shifrën e sëmundjes të paraqitur në formularin për pengesë për punë, përkatësisht se kolegia Ana ka dhimbje në shpinë ose tonzilitis. Informatat për sëmundjet janë të dhëna personale veçanërisht të ndjeshme (kategori e veçantë) dhe duhet të veprohet lidhur me to, në mënyrë të veçantë, dhe rekomandimi do të jetë që ato të dhëna të anonimizohen, ndërsa "qarkullimi" i këtyre të dhënave të raportohet menjëherë te Oficeri për mbrojtjen e të dhënave personale, i cili duhet t'i shohë shkaqet për humbjen e të dhënave dhe për atë ta njoftojë Agjencinë për Mbrojtjen e të Dhënave Personale (sipas vlerësimit ndoshta edhe subjekti për mbrojtjen e të dhënave personale), më së voni 72 orë pas ndodhjes së incidentit.

Detyra 6: Mbështetja dhe promovimi i "Mbrojtjes teknike dhe të integruar të të dhënave personale

Siç u cek edhe në fazat dhe detyrat paraprake, ju, si Oficer për mbrojtjen e të dhënave personale nevojitet që të konsultoheni për çështje nga sfera e mbrojtjes së të dhënave personale që dalin në kuadër të organizatës, përfshirë edhe për udhëzimet në aspekt të përgatitjes së politikave të përgjithshme etj.

Në pajtim me nenin 29 të LMDHP-së:

"Sipas arritjeve më të fundit teknologjike, shpenzimeve të realizimit, natyrës, qëllimit, kontekstit dhe qëllimeve të përpunimit, si dhe rreziqeve me probabilitet dhe seriozitet të ndryshëm për të drejtat dhe liritë e personave fizikë që rrjedhin nga përpunimi, kontrollori në momentin e përcaktimit të mjeteve për përpunim, si dhe në momentin e vetë përpunimit, është i detyruar t'i zbatojë masat e duhura teknike dhe organizative siç është pseudonimizimi, e që janë zhvilluar me qëllim zbatimin efektiv të parimeve të mbrojtjes së të dhënave personale siç është reduktimi në vëllim minimal të të dhënave dhe përfshirja e masave të nevojshme mbrojtëse në procesin e përpunimit, me qëllim përmbushjen e kërkesave të këtij ligji dhe sigurimin e mbrojtjes së të drejtave të subjekteve të të dhënave personale".

Kontrollori nevojitet që t'i zbatojë ato masa teknike dhe organizative që janë të nevojshme për aktivitete konkrete të përpunimit të të dhënave personale, përkatësisht, janë përshtatur për çdo qëllim të veçantë të përpunimit. Ky detyrim i referohet vëllimit të të dhënave personale të mbledhura, shkallës së përpunimit të tyre, periudhës së ruajtjes dhe qasshmnërisë në to.

Koncepti i përgjithshëm i termit "Data protection by design" mund të ndahet në "7 parime themelore", të cilat e theksojnë nevojën për të qenë proaktiv gjatë monitorimit të privatësisë, përkatësisht kërkesave nga faza e dizajnimit, dhe për kohëzgjatjen e të gjithë ciklit jetësor të të dhënave personale, të "inkorporohen në dizajnin dhe arkitekturën e sistemeve të TI-së dhe praktikat e punës...pa reduktuar funksionalitetin...", me privatësinë si cilësim standard, sigurinë (end-

to-end security) gjatë gjithë procesit, përfshirë dhe sigurimin e shkatërrimit të të dhënave dhe transparencës së fortë që i nënshtrohet verifikimit të pavarur. Parimi i privatësisë është nxjerrë si i dyti nga parimet themelore, duke përcaktuar që mbrojtja e të dhënave nga dizajni siguron që të dhënat personale të mbrohen automatikisht në të gjitha sistemet e TI-së ose praktikat e punës. Thjesht, subjekti gëzon automatikisht të drejtën themelore për privatësi dhe mbrojtjen e të dhënave personale.

Administrata publike është e thirrur të udhëhiqet në zbatimin e këtyre parimeve në mënyrë të përgjegjshme, e gatshme për të demonstruar zbatimin e tyre, nëse është e nevojshme, pranë organit mbikëqyrës kompetent.

Privatësia sipas default dhe design mund të lidhet me vlerësimin e ndikimit mbi mbrojtjen e të dhënave (nga Detyra 4); në drejtim të konstatimit se roli juaj është qendror në procesin e mbrojtjes së të dhënave personale dhe është me rëndësi kryesore në qasjen ndaj privatësisë sipas design. Për këto arsye, është e nevojshme të përfshiheni që në fillim, pra kur institucioni e planifikon sistemin për përpunimin e të dhënave personale, në mënyrë që të mund të mbështesni të gjithë aktorët përkatës, përkatësisht: udhëheqësit, pronarët e proceseve të punës dhe departamentet e TI-së dhe teknologjisë. Seti i aftësive që pritet t'i zotërojnë këto aktorë duhet të korrespondojë me kërkesat, përkatësisht të përfshijë edukim dhe trajnim të plotë mbi metodologjitë dhe teknologjitë e duhura (nëse është e nevojshme, përmes trajnimeve shtesë në vendin e punës) dhe përfshirje të plotë gjatë dizajnimit, zhvillimit, testimit dhe përshtatjes së të gjitha produkteve, shërbimeve dhe aktiviteteve të institucionit "të ndjeshëm ndaj privatësisë" (përfshirë prokurimet publike).

Duhet në veçanti të keni kujdes, ta këshilloni institucionin tuaj në procedurat e prokurimit publik për të nxitur pjesëmarrje të aplikantëve të cilët mund të "tregojnë" se produkti ose shërbimi i tyre është plotësisht në përputhje me GDPR-në, përkatësisht është inkorporuar "mbrojtja e të dhënave sipas default dhe në vetë design". Në këtë drejtim, duhet t'u jepet përparësi konkurruese këtyre aplikantëve ndaj atyre që produktet ose shërbimet e të cilëve nuk mund të tregohet se i përmbushin kërkesat.

Detyra 7: Marrëdhëniet me palët e treta (kontrollorë të përbashkët, kontrollor-kontrollor, kontrollor-përpunues si dhe klauzola për transferim të të dhënave personale)

Me qëllim të harmonizimit me LMDHP-në, e veçanërisht me qëllim të "tregohet" harmonizimi i tillë, kontrollorët duhet t'i rregullojnë marrëdhëniet me palët e treta e veçanërisht:

- të nënshkruhen kontrata ndërmjet organeve ose trupave publike, veçanërisht nëse bëhet fjalë për "kontrollorë të përbashkët" të aktiviteteve të caktuara për përpunim të të dhënave personale;

- të përgatiten kontrata relevante me kontrollorë dhe përpunues tjerë (siç janë klauzolat standarde të përcaktuara nga Agjencia për Mbrojtjen e të Dhënave Personale[27]) dhe
- të përgatiten kontrata standarde ose të miratuara veçmas për transferim të të dhënave personale[28].

Qëllimi kryesor është se të gjitha këto përgjegjësi që kanë të bëjnë me "dëshmimin e harmonizimit" janë obligim i kontrollorit. Por, në praktikë, prej Jush pritet që të përfshiheni ngushtë në mënyrë të drejtpërdrejtë në këto aktivitete.

Detyra 8: Veprimi ndaj kërkesave të subjekteve të të dhënave personale

Subjektet e të dhënave personale mund ta kontaktojnë oficerin për mbrojtjen e të dhënave personale në lidhje me të gjitha çështjet që kanë të bëjnë me përpunimin e të dhënave të tyre personale dhe për të realizuar të drejtat e tyre sipas kësaj Rregulloreje.

Subjektet e të dhënave personale që dëshirojnë të realizojnë cilëndo nga të drejtat e tyre – e drejta e qasjes, korrigjimit, fshirjes ("e drejta për t'u harruar"), kufizimi i përpunimit, transferimi i të dhënave, e drejta e kundërshtimit dhe në lidhje me vendimmarrjen dhe profilizimin e automatizuar – ose për çdo pyetje ose ankesë tjetër të përgjithshme në lidhje me mbrojtjen e të dhënave personale duhet normalisht t'i drejtohen fillimisht Oficerit. Punonjësit në institucionin duhet të njoftohen se në rast nëse marrin ndonjë kërkesë të tillë duhet ta informojnë detyrimisht Oficerin në mënyrë që ai të përfshihet në procedurën e realizimit të të drejtave të subjekteve të të dhënave personale.

Prandaj, është e nevojshme të publikohen të dhënat e kontaktit të oficerit nga institucioni që e ka emëruar dhe se kontrollori duhet doemos të sigurojë "që oficeri për mbrojtjen e të dhënave është i përfshirë, në mënyrë adekuate dhe të shpejtë, në të gjitha çështjet që kanë të bëjnë me mbrojtjen e të dhënave personale". Për ato arsye, nëse subjekti i të dhënave duhet t'i drejtohet edhe një personi tjetër në organizatën, p.sh. këshilltari i përgjithshëm ose drejtori ekzekutiv, ata duhet t'ia përcjellin kërkesën oficerit.

Për më tepër, statusi juaj i pavarur duhet të sigurojë që kërkesa, pyetja ose ankesa të zgjidhet nga ju – ose nga punonjës kompetentë, nën mbikëqyrjen tuaj – në mënyrën e duhur, pa paragjykime në favor të institucionit ose kundër subjektit të të dhënave personale. Sidoqoftë, nevojitet që vetë ta formoni ose ta kontrolloni përgjigjen ndaj subjektit të të dhënave personale të përgatitur nga një punonjës tjetër. Kjo, veçanërisht duhet të përfshijë që nëse subjekti i të dhënave nuk është i kënaqur me përgjigjen, ai ose ajo mund t'i drejtohet oficerit.

---

[27] Vendimi për përcaktimin e klauzolave kontraktuese standarde ndërmjet kontrollorëve dhe përpunuesve („Gazeta zyrtare e RMV-së, nr. 280 nga 15.12.2021)

[28] Klauzola kontraktuese standarde për transferim të të dhënave personale në vendet e treta („Gazeta zyrtare e RMV-së, nr. 280 nga 15.12.2021")

Kjo pasi subjektet e të dhënave personale kanë të drejtë të paraqesin kundërshtim në Agjencinë për Mbrojtjen e të Dhënave Personale. Më saktësisht, Agjencia është e autorizuar të:

"veprojë ndaj ankesave të paraqitura nga një subjekt i të dhënave ... dhe të hetojë, deri në shkallën e përshtatshme për lëndën e ankesës dhe ta njoftojë parashtruesin e ankesës për ecurinë dhe rezultatin e hetimit..."

Me ç'rast, do të ishte e logjikshme që të jeni gjithashtu të gatshëm për t'u përgjigjur kërkesave dhe ankesave nga organizatat përfaqësuese (p.sh. organizatat civile), në vend që vetëm nga subjektet e të dhënave personale.

Nga këndvështrimi i praktikave aktuale, duhet të pritet që Agjencia për mbrojtjen e të dhënave personale (si EDPS në raport me oficerët institucionalë të BE-së) do t'i inkurajojë subjektet e të dhënave personale që gjithmonë t'i drejtohen fillimisht kontrollorit, përkatësisht Oficerit, për të parë nëse çështja mund të hetohet dhe zgjidhet pa përfshirjen e Agjencisë, me kusht që oficeri të konsultohet me Agjencinë, nëse është e nevojshme. Më shumë për bashkëpunimin me AMDHP-në në pikën 11 - Bashkëpunimi me Agjencinë për Mbrojtjen e të Dhënave Personale.

Kjo e përforcon pozicionin tuaj të veçantë, i cili është një urë lidhëse midis kontrollorit dhe rregullatorit (AMDHP)

Detyra 9: Ndjekja e funksioneve për harmonizim përkatësisht përsëritje të aktiviteteve nga funksionet organizative

Termi "ndjekje" tregon qartë se ky është një aktivitet i vazhdueshëm.

Ju jeni përgjegjës për ndjekjen e harmonizimit me rregullat në fushën e mbrojtjes së të dhënave personale.

Ju si oficer jeni gjithashtu përgjegjës për rritjen e vetëdijes brenda institucionit, veçanërisht në mesin e punonjësve që janë të përfshirë drejtpërdrejt në aktivitetet e përpunimit të të dhënave personale.

Siç thotë EDPS:

"Sigurimi i harmonizimit në veçanti fillon me rritjen e vetëdijes. ... Oficeri luan rol të rëndësishëm në zhvillimin e njohurive për çështjet e mbrojtjes së të dhënave brenda institucionit/trupit."

Rritja e vetëdijes "stimulon qasje parandaluese efikase në vend të mbikëqyrjes represive të mbrojtjes së të dhënave."

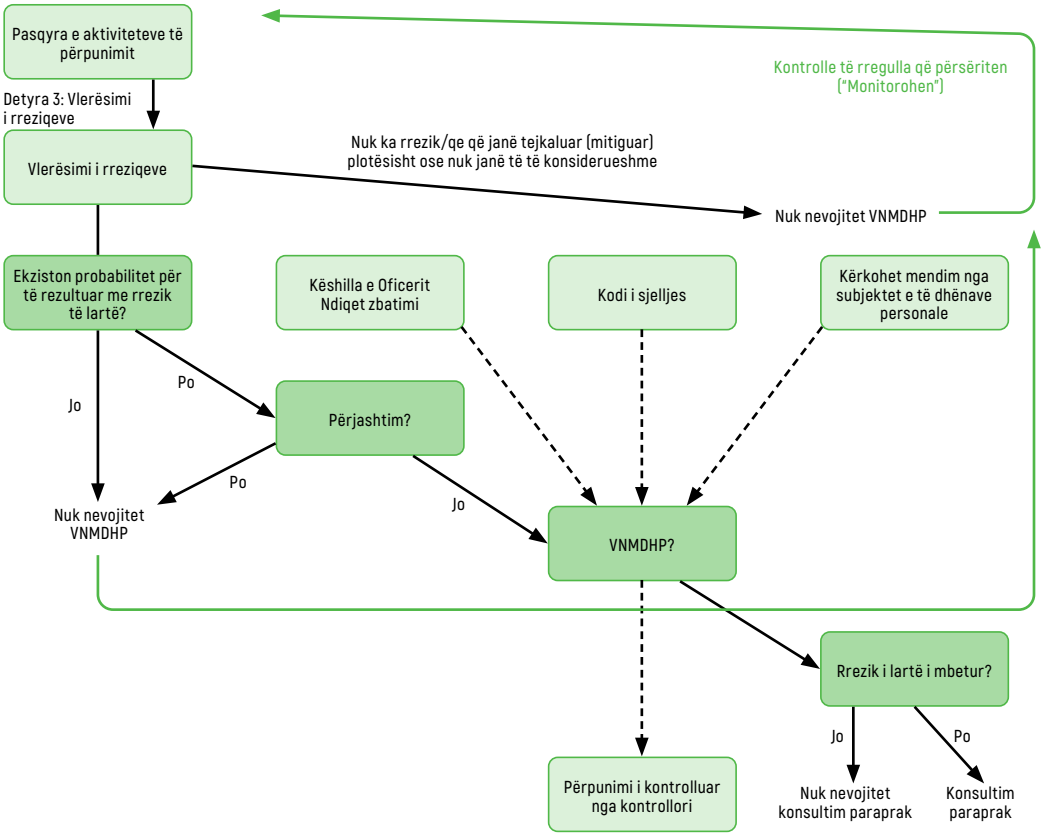
Gjegjësisht, nevojitet që ndjekja e harmonizimit të vërtetohet nga revizioni i jashtëm ose revizioni i brendshëm, përkatësisht personalisht nga Ju në rolin e oficerit, ose në bashkëpunim me funksione të tjera kryesore siç është PSSI (Personi përgjegjës për sigurinë e sistemit të informacionit).

Harmonizimi me mbrojtjen e të dhënave personale është përgjegjësi e Kontrollorit të të dhënave personale, e jo e oficerit. Por, nga Ju pritet, në bazë të rregullt, veçanërisht:

- të mblidhni informata që të identifikohen aktivitete të përpunimit të të dhënave personale,
- ta analizoni dhe kontrolloni harmonizimin e tyre dhe
- ta informoni, këshilloni dhe t'i lëshoni rekomandime kontrollorit ose përpunuesit.

Siç u theksua edhe në detyrën 4, lidhur me VNMDHP-në, nevojitet që të menaxhohet me rreziqet për të drejtat dhe liritë e personave fizikë, përkatësisht rreziqet duhet të identifikohen, analizohen, vlerësohen, evakuohen, trajtohen (p.sh., të zbuten) dhe monitorohen në mënyrë adekuate.

Detyra 2: Pasqyra e aktiviteteve të përpunimit të të dhënave personale



Shënimet tuaja duhet ta pasqyrojnë realitetin e aktiviteteve të përpunimit në Institucionin tuaj.

Kjo nënkupton që të dhënat personale të përditësohen rregullisht, veçanërisht kur institucioni juaj planifikon ndryshime në aktivitetet e përpunimit, për të cilat duhet të kontrolloni nëse shënimi duhet të përditësohet. Rekomandohet që ta përfshini formalisht këtë kontroll në procesin tuaj të menaxhimit të ndryshimeve. Pavarësisht ndryshimeve të planifikuara, rekomandohet që të realizohen kontrolle me qëllim të përcaktohen edhe ato të cilat ndoshta kanë mbetur të pavërejtura, por që duhet të përditësohen.

11.3. Funksioni këshillimor

Detyra këshillimore, në përgjithësi, zhvillohet në disa nivele:

- bartja e profesionalizmit Tuaj në udhëheqësinë që të mund të sigurohet harmonizimi gjatë realizimit të aktiviteteve për përpunim të të dhënave personale;
- përhapja e kulturës dhe rregullave për mbrojtje të të dhënave personale te të gjithë punonjësit/personat e angazhuar që përpunojnë të dhëna personale në kuadër të organizatës. Në atë mënyrë, do të keni mundësi t'i identifikoni çështjet kryesore ku kërkohet ndërhyrja Juaj ose qasja sistematike, për shembull për çdo:
  - propozim-vendim për krijim ose përplotësim të përpunimit ekzistues (veçanërisht që të sigurohet harmonizim me parimet për mbrojtje teknike dhe të integruar të të dhënave personale;
  - shqyrtimi i nevojës për vlerësim të ndikimit mbi mbrojtjen e të dhënave personale dhe për realizim të tij (me dokumentimin e mendimit tuaj në Raportin për realizim të VNMDHP-së);
  - monitorim të evidencës së aktiviteteve për përpunim të të dhënave personale;
  - dhënie të mendimit dhe përditësim të rregullave të brendshme ose politikave për mbrojtje të të dhënave personale;
  - propozim-masa që duhet të ndërmerren për cenim të sigurisë si dhe për njoftim të organit mbikëqyrës dhe subjektit të të dhënave personale;
  - Informim të subjekteve të të dhënave personale për të drejtat e tyre.

Ndërkaq veproni në drejtim të rritjes së vetëdijes dhe mbështetni punonjësit e çdo sektori/seksioni/njësie organizative në procedurën e përpunimit të të dhënave personale:

- nëpërmjet ndërtimit të kulturës të mbrojtjes së të dhënave personale (p.sh. mbajtja e edukimeve/trajnimeve/trajnimeve të brendshme mbi parimet themelore të mbrojtjes së të dhënave personale, etj.);

- nëpërmjet realizimit të aktiviteteve të komunikimit dhe rritjes së vetëdijes për tema të rëndësishme për organizatën (përdorimi i afisheve dhe udhëzuesve praktikë të disponueshëm në internet, rikujtimi i rregullave të sigurisë, fushatat e rreme për „fishing“, forma të tjera të inxhinierisë sociale, etj.);
- nëpërmjet përfaqësimit tuaj si pikë e brendshme kontakti për çdo çështje lidhur me mbrojtjen e të dhënave personale, dhe nëpërmjet ndërmjetësve (p.sh. punonjës me reputacion dhe njohje të mirë, në rolin e ambasadorëve për rritje të vetëdijes për mbrojtjen e të dhënave personale), nëse është e nevojshme.

Misioni juaj është pikërisht informimi, këshillimi dhe mbikëqyrja. Ju nuk jeni përgjegjës drejtpërdrejt për harmonizimin e organizatës, mbajtjen e evidencës, realizimin e vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale ose njoftimeve për shkelje të të dhënave personale. Megjithatë, pozita juaj është të jeni lojtar kryesor shkathtësitë e të cilit do të jenë të dobishme për personin udhëheqës të organizatës që t'i ndihmoni në procesin e harmonizimit me obligimet që dalin nga rregullat për mbrojtjen e të dhënave personale.

11.4. Funksioni i revizorit

Oficeri për mbrojtjen e të dhënave personale duhet të jetë i autorizuar, vetë ose me ndihmën e tjerëve të kryejë revizion/kontroll të kontrollorit me rregullat për mbrojtje të të dhënave personale. Për atë qëllim, kontrollori duhet t'ia sigurojë/japë të gjitha informatat dhe dokumentet e nevojshme të oficerit.

Vetëm procedura dhe mënyra e realizimit të revizioneve/kontrollorëve duhet të dokumentohet në aktin e brendshëm të kontrollorit.

Varësisht nga prioritetet, qëllimi i kontrolleve/revizioneve duhet të përbëhet prej:

- kontrollit të saktësisë së informatave të përfshira në evidencën e aktiviteteve për përpunim të implementuara nga instituti (regjistrimi i aktiviteteve për përpunim, qëllimi për përpunim, subjekte të të dhënave, natyra e të dhënave të përpunuara, marrës dhe transferime të jashtme të mundshme jashtë BE-së/Hapësirës ekonomike evropiane, afati i ruajtjes, masat e sigurisë dhe ngjashëm);
- kontrolleve të harmonizimit të aktiviteteve më të ndjeshme për përpunim, duke marrë parasysh vlerësimet e realizuara të ndikimit (veçanërisht lidhur me zbatimin e masave të dedikuara për zvogëlimin e probabilitetit dhe seriozitetit të rreziqeve);
- implementimit të mjeteve dhe kontrolleve periodike (analiza e privilegjeve, kontrolli i qasjes së autorizuar/të paautorizuar (loget), kontrolli i harmonizimit me afatet për ruajtje të të dhënave, etj.);

- monitorimit të efektivitetit të masave teknike dhe organizative për mbrojtjen e të dhënave personale të cilat organizata ka marrë përsipër të zbatojë.
- Rregullorja e sigurisë[29], për disa prej revizioneve/kontrolleve përcakton dinamikë të saktë të realizimit të tyre. Për tjerët për të cilat nuk është përcaktuar dinamikë e saktë, ju si oficer, përkatësisht kontrollor duhet të përcaktoni dinamikë për realizim, e cila do të bazohet në vlerësimin e rrezikut. Revizionet/kontrollet e përcaktuara në Rregulloren janë si në vijim:
- Kontrolli i evidencës për çdo qasje (logs) – **së paku njëherë në muaj**
- Kontrollori periodik i punës së administratorit të sistemit të informacionit
- Kontrollori vjetor (rishikimi) i dokumentit "Lista (pasqyra) me afate të ruajtjes së të dhënave personale"
- Kontrolli i privilegjeve për qasje – **së paku tremujor**
- Kontrolli i dokumentacionit për masa teknike dhe organizative – **së paku njëherë në vit**
- Kontrolli i brendshëm vjetor

Përfundimisht, duke marrë parasysh numrin dhe vëllimin e detyrave Tuaja, rekomandohet të përgatitni plan vjetor të aktiviteteve Tuaja, duke e marrë parasysh kohën e pritur për realizim dhe t'i merrni parasysh ngjarjet e reja, por edhe të kushtohet kohë për ngjarjet e paparapara; dhe të rishikohet dhe përditësohet rregullisht ky plan.

[29] („Gazeta zyrtare e RMV-së nr. 122 nga 12.5.2020")

12. BASHKËPUNIMI ME AGJENCINË

Oficeri ka për detyrë t'u përgjigjet kërkesave të Agjencisë për Mbrojtjen e të dhënave personale dhe atë në kuadër të sferës e cila është në kompetencë të saj, të bashkëpunojë me iniciativën e tij ose me iniciativën e Agjencisë.

Nga ju pritet të bashkëpunoni me Agjencinë për Mbrojtjen e të Dhënave Personale, si "lehtësues" në komunikim (duke u përgjigjur kërkesave gjatë mbikëqyrjes aty për aty, veprim pas pranimit të ankesës, pas konsultimeve në kuadër të realizimit të vlerësimit të ndikimit, pas njoftimit për shkeljen e të drejtës për mbrojtjen e të dhënave personale etj.).

Gjithashtu ekziston mundësia e konsultimit me Agjencinë për të gjitha çështjet që kanë të bëjnë me mbrojtjen e të dhënave personale apo vetë funksionin – oficeri për mbrojtjen e të dhënave personale.

Mbikëqyrjet e kryera nga Agjencia, aty për aty, mund të jenë me ose pa njoftim paraprak. Ndërkaq, pa marrë parasysh nëse mbikëqyrja është paralajmëruar ose jo, oficeri duhet të jetë i pranishëm kur ajo kryhet në ambientet e kontrollorit.

Raporti ndërmjet oficerit për mbrojtjen e të dhënave personale dhe Agjencisë për Mbrojtjen e të Dhënave Personale

Në gjendje ideale, roli i oficerit për mbrojtjen e të dhënave personale është të sigurojë harmonizim në kuadër të institucionit, përkatësisht të këshillojë ose veprojë në fazë të hershme, me qëllim shmangien e ndërhyrjes eventuale nga organi mbikëqyrës. Njëkohësisht, Agjencia për Mbrojtjen e të Dhënave Personale mund t'i ofrojë mbështetje të konsiderueshme oficerit në kryerjen e funksionit të tij.

Prandaj mbështetet ideja për zhvillim të sinergjisë ndërmjet oficerit dhe Agjencisë, e cila do të kontribuojë për arritjen e qëllimit të përgjithshëm për mbrojtje efikase të të dhënave personale në institucionet.

Sigurimi i harmonizimit

Sigurimi i harmonizimit fillon me rritjen e vetëdijes. Ju luani rol të rëndësishëm në zhvillimin e njohurisë për çështjet e mbrojtjes së të dhënave personale në kuadër të institucionit. Në të drejtim, organi mbikëqyrës e përshëndet veprimin parandalues në vend të mbikëqyrjes represive.

Gjithashtu, prej jush pritet të jepni këshilla në kuadër të institucionit tuaj, rekomandime praktike për përmirësimin e mbrojtjes së të dhënave personale ose interpretim lidhur me zbatimin e Rregullativës. Ky funksion është përshëndetur nga Agjencia për Mbrojtjen e të Dhënave Personale e cila i këshillon të gjitha institucionet/trupat vendore për çështjet që kanë të bëjnë me përpunimin e të dhënave personale. Gjithashtu, në tema të caktuara më të përgjithshme, sigurojnë edhe udhëzime për institucionet/trupat.

Kontrolle paraprake

Mendimet e lëshuara nga Agjencia për Mbrojtjen e të Dhënave Personale në kuadër të konsultimeve paraprake, dhe autorizimet e lëshuara paraprake, janë, gjithashtu, shkas për Agjencinë në drejtim të ndjekjes dhe sigurimit të harmonizimit me LMDHP-në.

Gjegjësisht, praktika e mirë e EDPS[30] tregon se para miratimit final të mendimit të Agjencisë për kontroll paraprak, mund t' dorëzohet draft i përkohshëm oficerit me informata për rekomandimet e planifikuara, që hap hapësirë për diskutim për efikasitetin dhe pasojat nga rekomandimet e planifikuara, me qëllim ato të jenë efikas dhe praktikë.

Zbatimi

Në pjesën e zbatimit të masave të caktuara për mbrojtjen e të dhënave personale, shfaqet një sinergji ndërmjet zyrtarit dhe Agjencisë, lidhur me miratimin e sanksioneve dhe veprimin ndaj ankesave dhe çështjeve.

Siç është përmendur tashmë, oficeri ka autorizime të kufizuara për realizim. Agjencia do të kontribuojë për sigurimin e harmonizimit me LMDHP-në, duke ndërmarrë masa efektive në aspekt të konsultimeve ose autorizimeve paraprake, përkatësisht ankesave dhe çështjeve tjera.

Masat mund të jenë efektive nëse janë të orientuara mirë dhe të realizueshme. Ju shiheni si një partner strategjik në përcaktimin e një aplikimi të orientuar mirë të masës.

Veprimi ndaj ankesave dhe çështjeve nga ju në nivel lokal inkurajohet, veçanërisht lidhur me fazën e parë të hetimit dhe zgjidhjes, përpara se të thirret Agjencia.

Gjithashtu, mund të konsultoheni me Agjencinë sa herë që keni dyshime për procedurën ose përmbajtjen e ankesave. Megjithatë, kjo nuk i pengon subjektet e të dhënave personale t'i drejtohen drejtpërdrejt Agjencisë.

Kompetencat e kufizuara të oficerit, nga ana tjetër, nënkuptojnë se në disa raste ankesa ose kërkesa duhet doemos të përshkallëzohet në Agjencinë. Prandaj, Agjencia ofron mbështetje të konsiderueshme në fushën e realizimit. Si kompensim, mund të mbështet në ju, në aspekt të sigurimit të informatave dhe ndjekjes së masave të miratuara.

Matja e efektivitetit

Lidhur me matjen e efektivitetit të zbatimit të kërkesave për mbrojtjen e të dhënave personale, ju jeni partner i dobishëm për të vlerësuar progresin në këtë fushë. Për shembull, kur bëhet fjalë për matjen e performancave të mbikëqyrjes së

[30] European Data Protection Supervisor

brendshme, Agjencia inkurajon t'i zhvilloni kriteret tuaja për kryerjen e mbikëqyrjes cilësore (standarde profesionale, plane specifike për institucionin, program vjetor të punës, etj.). Këto kritere, nga ana e tyre, do t'i mundësojnë Agjencisë, aty ku është e ftuar ta bëjë këtë, ta vlerësojë punën e oficerit, por do t'i mundësojë edhe ta matë gjendjen e zbatimit të LMDHP-së në kuadër të institucionit.

Është gjithashtu e mundshme që si oficer në sektorin publik të ftoheni nga Agjencia për të kontribuar në konsultimet që i zhvillon dhe të sigurojë kontribut të saj aktiv gjatë përgatitjes së mendimit formal për ligje të propozuara ose draft-ligje në sferën e mbrojtjes së të dhënave personale që i referohet pjesës të cilën e punon oficeri.

Kjo është shpesh me rëndësi kryesore, veçanërisht në lidhje me sistemet e ndëlikuara të përpunimit ku kërkohet njohuri e thelluar e arkitekturës së TI-së dhe proceseve të brendshme për kontroll të duhur.

Portali kombëtar për shërbime elektronike (uslugi.gov.mk)

Portali kombëtar për shërbime elektronike (në tekstin e mëtejmë: Portali) është platformë elektronike, e disponueshme në https://uslugi.gov.mk, përmes së cilës qytetarëve të RMV-së u mundësohet të marrin informacione për shërbimet publike dhe të përdorin shërbime elektronike nga organe kompetentë dhe institucione tjera që ofrojnë shërbime elektronike përmes Portalit.

Portali është krijuar dhe menaxhohet nga Ministria e Shoqërisë Informatike dhe Administratës (në tekstin e mëtejmë: MSHIA), e cila është përgjegjëse për disponueshmërinë dhe funksionimin teknik të Portalit, si dhe për sistemet me të cilat është i lidhur. Përmes Portalit, ofruesi i shërbimeve elektronike i shfrytëzon kërkesat për ofrimin e shërbimit administrativ në mënyrë elektronike të përcaktuara në përputhje me Ligjin, ndërsa ofruesi i shërbimeve elektronike i informon përdoruesit për shërbimet e kryera.

Bazën ligjore për funksionimin e Portalit e jep Ligji për menaxhim elektronik dhe shërbimet elektronike, ku është përcaktuar shkëmbimi elektronik i të dhënave dhe mënyra në të cilën duhet të realizohet, ofrimi i shërbimeve elektronike, funksionimi i ndërmjetësve etj.

Ligje të tjera të rëndësishme për funksionimin e Portalit janë Ligji për Regjistrin Qendror të Popullsisë dhe Ligji për dokumentet elektronike, identifikimin elektronik dhe shërbimet konfidenciale që sigurojnë realizimin e shërbimeve elektronike duke përdorur mjete të thjeshta për përdoruesin, përfshirë personat me aftësi të kufizuara.

Për përmbajtjen e informacioneve për shërbim të caktuar, si dhe për ofrimin e shërbimeve elektronike, përgjegjës është vetëm organi kompetent ose subjekt tjetër - ofrues i shërbimit.

Lidhur me të dhënat personale, si oficer keni për obligim të kujdeseni për mënyrën e mbledhjes, përpunimit dhe dhënies së të dhënave personale, në përputhje me ligjin.

Në këtë drejtim, duhet të jepen këshilla për zbatimin dhe përmbushjen e kërkesave minimale teknike, politikave dhe standardeve për sigurimin e qasjes në shërbimet elektronike të ofruesit të shërbimeve elektronike, të miratuara nga MSHIA-ja.

Në aspekt të formës elektronike të dokumenteve, nga organet kompetente, ato lëshohen në bazë të standardeve të përcaktuara nga ministri i Shoqërisë Informatike dhe Administratës.

Përpunimi i kërkesës në formë elektronike kryhet përmes portalit, ku ofruesi i shërbimeve elektronike i përdor të dhënat për përdoruesin të përfshirë në regjistrin e popullsisë dhe rregullat për mbrojtjen e të dhënave personale. Si përjashtim, nëse regjistri i popullsisë nuk i përmban të dhënat e nevojshme, ato sigurohet nga burimi i të dhënave prej ku tashmë janë mbledhur.

Të gjitha dokumentet e pranuara dhe të dorëzuara në formë elektronike ruhen në sistemin informativ të ofruesve të shërbimeve elektronike, në përputhje me ligjin.

Oficeri për mbrojtjen e të dhënave personale duhet të përfshihet në procesin e përcaktimit të marrëdhënieve të ndërsjella që kanë institucionet, veçanërisht kur bëhet fjalë për shkëmbimin elektronik të të dhënave dhe dokumenteve.

Nga organet e pushtetit shtetërore pritet të zbatojnë masa për sigurinë e sistemit informativ të cilin e përdorin për komunikim në formë elektronike, duke zbatuar standarde dhe rregulla të veçanta[31] të përcaktuara nga MSHIA-ja.

Rekomandohet që oficeri të jetë pjesë e ekipit përgjegjës për lidhjen e platformës për interoperabilitet nga institucioni dhe të informohet rregullisht për ndryshimet e mundshme të saj.

Inteligjenca artificiale dhe obligimet e OMDHP-së

Inteligjenca artificiale (IA) ngre pyetje të rëndësishme dhe urgjente. IA-ja tashmë është me ne – duke ndryshuar informatat që i marrim, zgjedhjet që i bëjmë dhe mënyrat në të cilat funksionon shoqëria jonë. Në vitet që vijnë do të luajë rol ende më të madh në atë se si organet shtetërore dhe institucionet publike funksionojnë dhe si komunikojnë qytetarët dhe si marrin pjesë në procesin demokratik.

Kjo sjell sfida të reja për OMDHP-në prej të cilit pritet ta analizojë dhe kuptojë mënyrën në të cilën punojnë sistemet për IA dhe implikimet potenciale të këtyre teknologjive, me ç'rast ai nuk ka zgjedhje përveç të mbetet në hap me trendin.

[31] Platforma për interoperabilitet.

Në vazhdim janë përgjigjet e disa prej pyetjeve që mund të lindin nga e lartpërmendura dhe që do t'ju ndihmojnë juve si oficer në rast të implementimit të sistemit të bazuar në IA nga institucioni juaj.

1. A i rregullon LMDHP-ja inteligjencën artificiale dhe mësimin makinerik?

Po, LMDHP-ja e rregullon IA-në dhe mësimin makinerik. LMDHP-ja i rregullon të gjitha format e teknologjisë të cilat i përpunojnë të dhënat personale. Si rregullativë e bazuar në rrezik, LMDHP-ja angazhohet për parimet që zbatohen pa dallim të kontekstit në të cilin përpunohen të dhënat personale.

2. A përfshin gjithmonë përpunimi automatik IA ose mësim makinerik?

Jo, ka shumë raste ku përpunimi automatik nuk përfshin IA ose mësim makinerik. Aktivitetet për përpunim të të dhënave personale shpesh janë "të automatizuara" pa përfshirje të IA-së ose mësimit makinerik. Për shembull, sistemi për menaxhim me dokumente (ang. Document Management System) përfshin përpunim automatik të të dhënave personale, pa përfshirje të domosdoshme të IA-së ose mësimit makinerik.

3. A përfshijnë gjithmonë IA-ja dhe mësimi makinerik përpunim të të dhënave personale?

Jo, sistemet për IA dhe mësim makinerik ndonjëherë nuk përfshijnë përpunim të të dhënave personale. Ato mund të përdoren për qëllime të ndryshme që mund të mos kenë lidhshmëri me të dhënat personale, siç janë, parashikimi i motit, ku të dhënat hyrëse mbahen nga matjet atmosferike nga sensorë ose të dhëna për optimizim të përdorimit të pesticideve dhe lëndëve ushqyese. Ndërkaq, ka më shumë instanca ku sistemet për IA dhe mësim makinerik nuk përpunojnë të dhëna personale.

4. A zbatohet ndonjë prej neneve të LMDHP-së konkretisht për IA ose mësimin makinerik?

LMDHP-ja zbatohet për gjithë përpunimin e të dhënave personale; ndërkaq gjithmonë kur sistemi për IA ose mësim makinerik përdoret për përpunimin e të dhënave personale zbatohet LMDHP-ja.

5. Unë jam OMDHP. A duhet të angazhohem për rritjen e IA-së dhe mësimit makinerik?

Si oficer për mbrojtjen e të dhënave personale duhet të jeni të shqetësuar për rritjen e IA-së dhe mësimin makinerik, sepse këto teknologji mund të çojnë në miratimin automatik të vendimeve që potencialisht mund të kenë implikime serioze mbi të drejtat dhe liritë e subjekteve të të dhënave personale. Për shembull, IA-ja mund të përdoret për vendin automatik lidhur me skriningun e kandidatëve për

punësim. Të kuptuarit e mënyrës në të cilën funksionojnë algoritmet ju ndihmon të identifikoni rreziqe potenciale (lidhur me mbrojtjen e të dhënave personale) dhe të implementoni masa mbrojtëse adekuate, ku është e nevojshme.

Pa marrë parasysh madhësinë e institucionit, ju, si OMDHP, do të afektoheni nga integrimi i IA-së dhe mësimi makinerik në sistemet e TI-së së institucionit tuaj. Për shembull, aplikacionet në vijim përdorin IA ose planifikojnë ta përdorin në të ardhmen:

- Microsoft Office planifikojnë të kenë IA dhe mësim makinerik duke filluar (2023);
- Shumë softuerë për resurse njerëzore, përllogaritja e rrogave, shitja etj, tashmë përdorin IA dhe mësim makinerik, ndërsa ato që nuk kanë tashmë kanë plan të implementojnë;
- Chatbotet që përdorin të dhëna personale të personave fizikë për të dhënë përgjigje të personalizuara.

Si OMDHP, ju dhe ekipi juaj duhet të bëni vlerësim të ndikimit mbi mbrojtjen e të dhënave personale (VNMDHP) për të gjitha aktivitetet e reja të përpunimit. Me realizimin e tij, është veçanërisht e rëndësishme të kuptohen implikimet dhe kufizimet e sistemeve të IA-së, veçanërisht nëse ekzistojnë çfarëdo paragjykime. Gjithashtu, merret parasysh potenciali që sistemi i IA-së të gjenerojë rezultate të pasakta.

Si një OMDHP që punon për një organizatë e cila zbaton sistem për IA, ju duhet të keni rol në procedurën e menaxhimit të rrezikut të sistemeve për IA. Meqenëse një nga kërkesat e LMDHP-së është zbatimi i mbrojtjes së të dhënave personale by design dhe by default, një nga detyrat e OMDHP-së është t'i identifikojë, zvogëlojë ose zbusë rreziqet e njohura dhe të parashikueshme përmes dizajnit dhe zhvillimit adekuat të çdo sistemi për IA i cili përpunon të dhëna personale.

6. Cilët janë bisedimet kryesore që duhet t'i zhvilloj brenda në organizatën që të përgatitemi për zhvillimin e shpejtë të IA-së dhe mësimit makinerik?

Oficeri për mbrojtjen e të dhënave personale duhet të punojë së bashku me palët tjerë të prekur në institucionin, ku janë profesionistët TI, ekspertët juridikë si dhe përgjegjësit e sektorëve/shërbimeve që të formojnë rrjet për komunikim përmes IA-së. Ky rrjet për komunikim do të sigurojë që përdorimi i teknologjisë së IA-së dhe sistemet për IA në institucionin të jenë transparentë, llogaridhënës dhe të drejtë, por, mbi të gjitha, që përdorimi i IA-së të jetë i harmonizuar me LMDHP-në.

Në vazhdim janë disa hapa të cilat OMDHP-ja dhe anëtarët në rrjetin e komunikimit mund t'i ndërmarrin që të përgatiten për përdorimin e rritur të sistemeve për IA në organizatën:

- Të kuptuarit e teknologjisë së IA-së: Ju si OMDHP duhet të keni njohuri të mirë të teknologjisë të IA-së që përdoret nga organizata juaj. Kjo njohuri ndihmohet nga palët e interesuara që janë pjesë e rrjetit tuaj të komunikimit, me qëllim për të kuptuar teknologjitë e IA-së specifike për seksionet ku përdoren ato, duke përfshirë mënyrën se si funksionojnë, çfarë të dhënash mbledhin dhe përpunojnë dhe çfarë lloje vendimesh mund të sjelin vetë sistemet e IA-së.
- Specifikimi dhe dokumentimi i duhur i qëllimeve të përpunimit lidhur me sistemet e IA-së: kjo është shumë e rëndësishme si për fazën e projektimit ashtu edhe për fazën e zhvillimit të sistemit të ri të IA-së, me qëllim të zbatimit të parimeve të LMDHP-së, siç janë vëllimi minimal i të dhënave dhe mbrojtja e të dhënave personale. by design dhe by default , veçanërisht për sistemet e IA-së që përpunojnë një kategori të veçantë të të dhënave personale, siç janë të dhënat për gjendjen shëndetësore.
- Kryerja e vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale (VNMDHP): kryerja e VNMDHP-së është proces që ndihmon në identifikimin dhe minimizimin e rreziqeve për të dhënat personale. VNMDHP-ja duhet doemos të realizohet pavarësisht nëse përpunimi i të dhënave personale do të rezultojë me rrezik të lartë për të drejtat dhe liritë e subjekteve të të dhënave personale. OMDHP-ja duhet të punojë në bashkëpunim me palët e interesuara (anëtarët në rrjetin e komunikimit) për t'i identifikuar ndikimet e mundshme mbi privatësinë e personave fizikë dhe të drejtat e tyre. Pjesë kryesore e VNMDHP-së për sistemet e IA-së është të kontrollohen çfarëdo anshmëri të cilët mund të çojnë në diskriminim.
- Shqyrtimi i kontratave për përpunim të të dhënave personale: Ju si OMDHP duhet t'i shqyrtoni të gjitha kontratat e përpunimit të të dhënave personale me provajderët e IA-së për të siguruar që ato përfshijnë masa mbrojtëse adekuate për përpunimin e të dhënave personale nga sistemet e IA-së.
- Zbatimi i masave adekuate të sigurisë: Ju si OMDHP duhet të siguroheni që të zbatohen masat e duhura të sigurisë për të mbrojtur të dhënat personale nga qasja e paautorizuar, humbja ose shkatërrimi gjatë përdorimit të sistemeve për IA.
- Monitorimi dhe revizioni i sistemeve të IA-së: Ju si OMDHP duhet të menaxhoni dhe reviziononi sistemet e IA-së në bazë të rregullt për t'u siguruar që ato funksionojnë siç është paraparë dhe se rreziqet ndaj të dhënave personale menaxhohen në mënyrë efektive.

Efekti i inteligjencës artificiale mbi të drejtat e njeriut

Dinjiteti i pacenueshëm dhe i lindur i çdo njeri e përbën bazën për një sistem universal, të pandashëm, të patjetërsueshëm, dhe të ndërvarur dhe të ndërlidhur të të drejtave dhe lirive themelore të njeriut. Prandaj, respektimi, mbrojtja dhe avancimi i dinjitetit dhe të drejtave të njeriut siç është përcaktuar me të drejtën ndërkombëtare, përfshirë edhe të drejtën ndërkombëtare për të drejtat e njeriut, është me rëndësi esenciale gjatë ciklit jetësor të sistemeve për inteligjencë artificiale. Dinjiteti i njeriut ka të bëjë me njohjen e vlerës së brendshme dhe të barabartë të çdo qenie njerëzore, pa dalim të racës, ngjyrës, origjinës, gjinisë, moshës, gjuhës, religjionit, mendimit politik, origjinës kombëtare, origjinës etnike, origjinës sociale, gjendjes ekonomike ose sociale, lindjes ose invaliditetit dhe cilado bazë tjetër.

Asnjë qenie njerëzore apo komunitet njerëzor nuk duhet të dëmtohet apo të jetë e vartëse (qoftë në aspektin fizik, ekonomik, social, politik, kulturor apo mendor) gjatë cilësdo faze të ciklit jetësor të sistemeve të IA-së. Gjatë gjithë ciklit jetësor të sistemeve të IA-së cilësia e jetës së njerëzve duhet të përmirësohet, ndërsa përkufizimi i "cilësisë së jetës" duhet të lihet i hapur për individët ose grupet, për sa kohë që nuk ka shkelje ose keqpërdorim të të drejtave dhe lirive themelore të njeriut ose dinjiteti njerëzor në kuptim të këtij përkufizimi[32].

Personat mund të komunikojnë me sistemet e inteligjencës artificiale gjatë ciklit të tyre jetësor dhe të marrin ndihmë prej tyre, si për shembull kujdesi për njerëzit vulnerabilë ose njerëzit në situata vulnerabile, përfshirë, por pa u kufizuar në fëmijët, të moshuarit, njerëzit me aftësi të kufizuara ose të sëmurët. Në kuadër të ndërveprimeve të tilla, personat nuk duhet të objektivizohen asnjëherë, as nuk duhet të minohet dinjiteti i tyre në mënyrë tjetër apo të cenohen apo keqpërdoren të drejtat dhe liritë themelore të njeriut.

Të drejtat dhe liritë themelore të njeriut duhet të respektohen, mbrohen dhe promovohen gjatë gjithë ciklit jetësor të sistemeve të inteligjencës artificiale. Institucionet shtetërore, sektori privat, shoqëria civile, organizatat ndërkombëtare, komuniteti akademik duhet t'i respektojnë kornizat e të drejtave të njeriut në proceset rreth ciklit jetësor të sistemeve për IA. Teknologjitë e reja duhet të ofrojnë mjete të reja për përfaqësimin, mbrojtjen dhe realizimin e të drejtave të njeriut, e jo për shkeljen e tyre.

Privatësia, si një e drejtë thelbësore për mbrojtjen e dinjitetit njerëzor dhe autonomisë njerëzore, duhet të respektohet, mbrohet dhe promovohet gjatë gjithë ciklit jetësor të sistemeve për IA. Është e rëndësishme që të dhënat e sistemeve të IA-së të mblidhen, përdoren, ndahen, arkivohen dhe fshihen në mënyra që janë në përputhje me të drejtën ndërkombëtare, duke i respektuar kornizat ligjore përkatëse kombëtare, rajonale dhe ndërkombëtare.

32

Duhet të vendosen korniza adekuate për mbrojtjen e të dhënave dhe mekanizmave për menaxhim me qasjen nga më shumë palë të interesuara në nivel kombëtar ose ndërkombëtar, të mbrojtura nga sistemet gjyqësore dhe të siguruara gjatë gjithë ciklit jetësor të sistemeve të IA-së.

IA-ja përfshin mundësi por edhe rreziqe për të drejtat e njeriut të cilat duhet të mbrohen, e jo të rrezikohen nga vetë sistemet e IA-së. Këto rekomandime për IA-në dhe të drejtat e njeriut ofrojnë udhëzime për mënyrën në të cilën ndikimi negativ i sistemeve të IA-së mbi të drejtat e njeriut mund të parandalohen ose zbuten, duke u fokusuar në 10 fushëveprime kryesore.

1. Vlerësimi i ndikimit mbi të drejtat e njeriut

Është e nevojshme të vendoset kornizë ligjore e cila e përcakton procedurën që institucionet shtetërore të jenë në gjendje të kryejnë vlerësim të ndikimit mbi të drejtat e njeriut (në tekstin e mëtejmë: VNDNJ) të sistemeve për IA të fituara, të zhvilluara dhe/ose të përdorura nga këto institucione. VNDNJ-ja duhet të realizohet dhe/ose të përdoret në mënyrë të ngjashme me format e tjera të vlerësimit të ndikimit të kryera nga institucionet shtetërore, si vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale. Organi mbikëqyrës mund të përcaktojë se cilat lloje të sistemeve për IA janë objekt i VNDNJ-së, por ato sisteme të përcaktuara për IA doemos duhet t'i përfshijnë të gjitha sistemet e IA-së që kanë potencialin të ndikojnë mbi të drejtat e njeriut në çdo fazë të ciklit jetësor të sistemit për IA.

Si pjesë e kornizës ligjore të VNDNJ-së, nga institucionet shtetërore duhet të kërkohet të kryejnë vetëvlerësim të sistemeve ekzistuese dhe të propozuara për IA. Ky vetëvlerësim duhet të vlerësojë ndikimin e mundshëm të të drejtave të njeriut të sistemit të IA-së duke marrë parasysh natyrën, kontekstin, fushëveprimin dhe qëllimin e sistemit. Nëse institucioni shtetëror nuk ka blerë apo zhvilluar ende sistem për IA, ky vlerësim duhet të kryhet përpara blerjes dhe/ose zhvillimit të atij sistemi.

VNDNJ-ja duhet të përfshijë gjithashtu revizion të jashtëm të sistemeve të IA-së, qoftë nga një organ i pavarur ose një revizor të jashtëm me ekspertizë përkatëse, për të ndihmuar në zbulimin, matjen dhe/ose hartëzimin e ndikimit dhe rreziqeve të të drejtave të njeriut që do të lindin.

Vetëvlerësimi dhe revizioni i jashtëm nuk duhet të kufizohen në vlerësimin e modeleve ose algoritmeve pas sistemeve për IA, por duhet të përfshijnë gjithashtu vlerësim se si vendimmarrësit mund të mbledhin ose ndikojnë në parametrat e hyrjes, si dhe të interpretojnë parametrat e prodhimit të një sistemi të tillë. Ai gjithashtu duhet të përfshijë vlerësim nëse sistemi për IA mbetet nën kontroll të konsiderueshëm njerëzor gjatë gjithë ciklit jetësor.

Në rrethanat kur vetëvlerësimi ose revizioni i jashtëm zbulon se sistemi për IA përbën rrezik real të shkeljeve të të drejtave të njeriut, VNDNJ-ja duhet t'i

përcaktojë masat mbrojtëse dhe mekanizmat që ekzistojnë për të parandaluar ose zbutur atë rrezik. Në rrethanat kur një rrezik i tillë është identifikuar në lidhje me sistemin për IA që tashmë është vënë në përdorim nga institucionet shtetërore, përdorimi i tij duhet të pezullohet menjëherë derisa të zbatohen masat mbrojtëse dhe mekanizmat e lartpërmendur. Aty ku nuk është e mundur të zbuten në mënyrë të konsiderueshme rreziqet e identifikuara, sistemi për IA nuk duhet të vihet në përdorim ose të përdoret nga cilido institucion shtetëror. Atje ku vetëvlerësimi ose revizioni i jashtëm zbulon shkelje të të drejtave të njeriut, institucioni shtetëror duhet të veprojë menjëherë për të mënjanuar shkeljen dhe të ndërmarrë masa për të parandaluar ose zbutur rrezikun nëse ndodh përsëri një shkelje e tillë.

VNDNJ-ja, përfshirë konstatimet nga hulumtimi ose konkluzionet nga revizioni i jashtëm, doemos duhet të jetë e disponueshme për publikun me format të disponueshëm lehtësisht dhe me format të lexueshëm makinerik.

Institucionet shtetërore nuk duhet të prokurojnë sisteme për IA nga palët e tretë në rrethana kur pala e tretë nuk është e përgatitur të tërhiqet nga kufizimet për dorëzim të informatave (p.sh., konfidencialitet ose sekrete pune) dhe kur kufizimet e tilla e pengojnë procesin e: realizimit të VNDNJ (përfshirë edhe realizimin e revizionit të jashtëm) dhe publikimit të VNDNJ-së.

Institucionet shtetërore duhet të realizojnë rregullisht VNDNJ dhe atë jo vetëm ku institucionet shtetërore prokurojnë dhe/ose zhvillojnë sisteme të IA-së. VNDNJ-ja duhet, së paku, të realizohet gjatë çdo faze të re të ciklit jetësor të sistemit për IA dhe gjatë ndryshimeve të konsiderueshme të ngjashme.

2. Konsultime publike

Përdorimi i sistemeve për IA nga institucionet shtetërore duhet të menaxhohet nga standardet për prokurim të hapur, të zbatuara në procesin transparent ku të gjitha palët e prekura relevante janë ftuar të japin kontributin e tyre.

3. Obligimet për lehtësim të implementimit të standardeve për mbrojtje të të drejtave të njeriut në sektorin privat

Nevojitet që shteti të implementojë masa në përputhje me Konventën Evropiane për të Drejtat e Njeriut[33], për aktorët e IA-së (p.sh., kreatorët e IA-së, provajderët etj.) të mund t'i implementojnë ato principe (parime) gjatë punës së tyre.

4. Informatat dhe transparenca

Duhet të njihet përdorimi i një sistemi të IA-së në çdo proces vendimmarrjeje që ka ndikim të konsiderueshëm mbi të drejtat e njeriut. Jo vetëm që është i nevojshëm përdorimi i sistemeve të IA-së duhet të shpallet publikisht (duke përdorur terma të qarta dhe të disponueshme), individët, gjithashtu, duhet doemos të jenë të aftë të kuptojnë se si merren vendimet dhe si verifikohen ato vendime.

[33] European Convention on Human Rights.

Nëse sistemi i IA-së përdoret për të ndërvepruar me individë në kontekstin e shërbimeve publike, veçanërisht drejtësisë dhe kujdesit shëndetësor, është e nevojshme që përdoruesi të njoftohet dhe të komunikohet pa e prolonguar mundësinë për të kërkuar ndihmë ose mbrojtje nga personi profesional.

Duhet të mundësohet revizion i sistemit të IA-së, në lidhje me kërkesat e transparencës. Kjo mund të jetë ose në formën e zbulimit publik të informatave për sistemin në fjalë, proceset e tij, efektet e drejtpërdrejta dhe të tërthorta mbi të drejtat e njeriut dhe masat e ndërmarra për të identifikuar dhe zbutur ndikimet negative mbi të drejtat e njeriut, ose në formën e një revizioni të pavarur, gjithëpërfshirës dhe efektiv. Në të gjitha rastet, informatat e disponueshme duhet të mundësojë një vlerësim kuptimplotë të sistemit të IA-së. Asnjë sistem i IA-së nuk duhet të jetë kompleks deri në atë shkallë në të cilën nuk mundëson kontroll dhe verifikim njerëzor. Sistemet që nuk mund të jenë objekt i standardeve adekuate të transparencës dhe përgjegjësisë nuk duhet të përdoren.

5. Mbikëqyrja e pavarur

Trupat mbikëqyrës duhet të jenë të pavarur nga institucionet shtetërore dhe kompanitë private që zhvillojnë, vënë në përdorim ose në mënyrë tjetër i përdorin sistemet për IA-së dhe ato doemos duhet të jenë të pajisura me ekspertizë adekuate ndërdisiplinore, kompetenca dhe resurse për kryerjen e funksionit të tyre mbikëqyrës.

Trupat e pavarur mbikëqyrës duhet ta hulumtojnë dhe monitorojnë në mënyrë proaktive harmonizimin e sistemeve për IA me të drejtat e njeriut, të pranojnë dhe të veprojnë ndaj ankesave nga palët e interesuara, të kontrollojnë periodikisht aftësitë dhe zhvillimin teknologjik të sistemeve për IA. Ato duhet ta kenë fuqinë për të ndërhyrë në gjendjet kur ato identifikojnë (rrezik nga) shkelje të të drejtave të njeriut.

6. Barazia dhe mosdiskriminimi

Në të gjitha rrethanat, rreziqet nga diskriminimi doemos duhet të pengohen dhe zbuten me vëmendje të veçantë për grupet që kanë rrezik të shtuar mbi të drejtat e njeriut, e ato janë nën ndikimin e IA-së.

Kjo i përfshin gratë, fëmijët, më të vjetrit, personat të rrezikuar ekonomikisht, personat me aftësi të kufizuara dhe grupet "racore", etnike ose religjioze.

7. Mbrojtja e të dhënave personale dhe privatësisë

Zhvillimi, trajnimi, testimi dhe përdorimi i sistemeve për IA që mbështeten në përpunimin e të dhënave personale doemos duhet ta sigurojnë plotësisht të drejtën e respektimit të jetës private dhe familjare sipas nenit 8 të Konventës Evropiane për të drejtat e Njeriut, përfshirë edhe "të drejtën e vetëvendosjes së informuar" lidhur me të dhënat e tyre.

Përpunimi i të dhënave në kontekst të sistemeve për IA do të jetë proporcionale lidhur me qëllimin legjitim që realizohet përmes përpunimit të tillë. Në të gjitha fazat duhet të ekzistojë balancë e drejtë ndërmjet interesave që realizohen përmes zhvillimit dhe vënies në përdorim të sistemeve për IA dhe të drejtave dhe lirive të personave fizikë.

Përpunimi i të dhënave personale në cilëndo fazë të ciklit jetësor të sistemit për IA doemos duhet të bazohet në parimet e cekura më poshtë nga Konventa 108+[34], e veçanërisht:

i. duhet doemos të ekzistojë bazë legjitime për përpunim në përputhje me Ligjin për mbrojtjen e të dhënave personale në fazat e duhura të ciklit jetësor të sistemit të IA-së;

ii. të dhënat personale duhet doemos të përpunohen në mënyrë të ligjshme, të drejtë dhe transparente;

iii. të dhënat personale duhet doemos të mblidhen për qëllime të qarta, të specifikuara dhe legjitime dhe të mos përpunohen në një mënyrë e cila është jokompatibile me ato qëllime;

iv. të dhënat personale duhet doemos të jenë të përshtatshme, relevante dhe të mos jenë tej mase lidhur me qëllimet për të cilat ato përpunohen;

v. të dhënat personale duhet doemos të jenë të sakta dhe, ku është e nevojshme, të përditësohen;

vi. të dhënat personale duhet të ruhen në një formë që lejon identifikimin e subjekteve të të dhënave personale jo më gjatë se sa që është e nevojshme për qëllimet për të cilat përpunohen ato të dhëna.

8. Liria e shprehjes, liria e mbledhjes dhe bashkimit dhe e drejta e punës

Në kontekst të përgjegjësive të tyre t'i respektojnë, mbrojnë dhe përmbushin të gjitha të drejtat dhe liritë themelore të njeriut, duhet të merret parasysh gjithë spektri i standardeve ndërkombëtare për të drejtat njeriut që mund të përfshihen me përdorimin e IA-së.

- Liria e shprehjes: Duhet të mendohet për ndërmarrjen e masave adekuate për rregullim të monopoleve teknologjike për të parandaluar efektet negative nga përqendrimi i ekspertizës dhe fuqisë së IA-së mbi rjedhën e lirë të informacionit.
- Liria e mbledhjes dhe e bashkimit: Theks i veçantë duhet vënë në ndikimin që mund të ketë përdorimi i sistemeve të IA-së në lirinë e mbledhjes dhe shoqërimit, veçanërisht në kontekstet ku këto liri janë të vështira për t'u realizuar offline.

[34] Convention 108+ for the protection of individuals with regard to the processing of personal data.

- E drejta e punës: Potenciali i IA-së për të përshpejtuar automatizimin dhe në këtë mënyrë të ndikojë negativisht mbi mundësinë e punës duhet të monitorohet me kujdes. Duhet të bëhen vlerësime të rregullta për të monitoruar numrin dhe llojet e vendeve të punës të krijuara dhe të humbura për shkak të zhvillimit të inteligjencës artificiale.

9. Mjeti për arritjen e drejtësisë (eng. Remedies)

Sistemet për IA doemos duhet të mbeten nën kontrollonin e njeriut, bile edhe në rrethana ku mësimi makinerik ose teknikat e ngjashme mundësojnë që sistemet për IA të miratojë vendim në mënyrë të pavarur nga ndërhyrja specifike e njeriut. Duhet doemos të vendosen linja të qarta të përgjegjësisë për shkelje të të drejtave të njeriut që mund të paraqiten në faza të ndryshme të ciklit jetësor të sistemit për IA. Përgjegjësia dhe llogaridhënia për shkelje të të drejtave të njeriut ndodhin në zhvillimin, vënien në përdorim ose përdorimin e sistemeve për IA gjithmonë doemos duhet të jenë në duart e personit fizik, bile edhe në rastet kur masa me të cilën shkelen të drejtat e njeriut nuk është aplikuar drejtpërdrejt nga personi përgjegjës.

10. Edukimi për IA

Dija dhe njohuria për IA duhet të promovohet në institucionet shtetërore, organet e pavarura mbikëqyrëse, gjyqësorin, si dhe në publik.

Ata që janë të përfshirë drejtpërdrejt ose tërthorazi në zhvillimin ose aplikimin e sistemeve të IA-së duhet të kenë dijen dhe njohurinë e nevojshme se si funksionon sistemi i IA-së dhe të jenë të informuar për ndikimin e tij mbi të drejtat e njeriut. Në mënyrë që aktorë të tillë të informohen për ndikimin e sistemeve të tyre mbi të drejtat e njeriut, ata duhet gjithashtu të jenë të vetëdijshëm për gamën e standardeve të të drejtave të njeriut që janë duke u miratuar.

Shteti duhet të investojë në përmirësimin e nivelit të edukimit te publiku, dhe në lidhje me IA-në, përmes përpjekjeve të forta për rritjen e vetëdijes, trajnimit dhe edukimit, përfshirë edhe (veçanërisht) në shkollat. Kjo nuk duhet të kufizohet vetëm në edukimin lidhur me mënyrën në të cilën funksionon IA, por edhe për ndikimin e saj të mundshëm – pozitiv dhe/ose negativ – mbi të drejtat e njeriut. Duhet të bëhen përpjekje të veçanta për të prekur edhe grupet e margjinalizuara dhe ato që janë privuar nga e drejta lidhur me edukimin e TI-së.[35]

Në Shtojcën 7 është dhënë propozim çeking-lista për fushëveprimet e lartpërmendura.

[35] https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

PJESA 4 – SHTOJCA

SHTOJCA 1 – PROPOZIM-EVIDENCA E AKTIVITETEVE PËR PËRPUNIM TË TË DHËNAVE PERSONALE (KONTROLLORI DHE PËRPUNUESI)

EKZEMPLAR FORMAT TË EVIDENCËS PËR PËRPUNIM TË TË DHËNAVE PERSONALE TË KONTROLLORIT

Shënim: *Duke e pasur parasysh se nevojitet të përgatitet shënim i veçantë për çdo aktivitet për përpunim të të dhënave personale.*

Pjesa 1 – Informatat për kontrollorin

DETAJE PËR KONTAKT TË KONTROLLORIT: Emri, adresa, posta elektronike Telefoni
DETAJE PËR KONTAKT PËR KONTROLLORIN E PËRBASHKËT[36]:* Emri, adresa, posta elektronike Telefoni
DETAJE PËR KONTAKT PËR PËRFAQËSUESIN:* Emri, adresa, posta elektronike Telefoni
(*) Nëse është e aplikueshme DETAJE PËR KONTAKT TË OFICERIT PËR MBROJTJEN E TË DHËNAVE PERSONALE: Emri, adresa, posta elektronike, telefoni

Pjesa 2 – Të dhënat themelore për aktivitetet për përpunim të të dhënave personale

1. Emri i aktivitetit	
2. Njësia përgjegjëse („posedues i procesit të punës“)	
3. Qëllimi i përpunimit	
4. Kategori të subjekteve të të dhënave personale	

[36] Kini parasysh se është gjithnjë më e vështirë është të dallohen plotësisht përpunuesit nga kontrollorët. Shpesh, përpunuesit (që veprojnë në përputhje me udhëzimet e marra nga kontrollori, i cili i ka përcaktuar mjetet dhe qëllimet) tani marrin përsipër shumë më tepër përgjegjësi dhe mund të bëhen „kontrollorë të përbashkët“. Ky është veçanërisht rast me ofruesit e shërbimeve cloud – nga të cilët ofrojnë „Inteligjencë artificiale dhe mësim makinerik (AI/ML) nëpërmjet Machine-Learning-as-a-Service (MLaaS)“.
Në përputhje me diskutimet në detyrën preliminare, aranzhmanet ndërmjet subjekteve të përfshira në aranzhmanet e tilla të ndërlikuara duhet të evidentohen në mënyrë të qartë dhe të duhur. Formularët që i shënojnë aktivitetet e përpunimit duhet të përshtaten me aranzhmanet specifike.

5. Kategori të të dhënave personale	
6. Kategori të përdoruesve të cilëve u janë zbuluar ose do t'u zbulohen të dhënat personale	
7. A janë transferuar të dhënat në vend të tretë ose te organizatë ndërkombëtare?	
8. Në rast të transferimit të të dhënave personale: Cilat masa adekuate mbrojtëse janë siguruar?	
9. Afati i fshirjes	
10. Përshkrimi i përgjithshëm i masave të zbatuara teknike dhe organizative (të sigurisë)	
11. Baza ligjore *	

*Baza ligjore nuk është e detyrueshme, por praktika më e mirë tregon se është mirë të ceket në evidencë.

EKZEMPLAR FORMATI I EVIDENCËS PËR PËRPUNIM TË TË DHËNAVE PERSONALE TË PËRPUNUESIT

Duke e pasur parasysh se doemos duhet të ekzistojë shënim për çdo aktivitet për përpunimin e të dhënave personale, për çdo kontrollor të veçantë.

Informata për përpunuesin dhe cilido nënpërpunues

DETAJE PËR KONTAKT TË PËRPUNUESIT: Emri, adresa, posta elektronike, telefoni
DETAJE PËR KONTAKT PËR OFICERIN PËR MBROJTJE TË DHP: Emri, adresa, posta elektronike, telefoni
DETAJE PËR KONTAKT PËR NËNPËRPUNUESIN:* Emri, adresa, posta elektronike, telefoni
(*) Nëse është e aplikueshme DETAJE PËR KONTAKT TË OFICERIT PËR MBROJTJE TË TË DHP: Emri, adresa, posta elektronike, telefoni

(*) nëse është e aplikueshme

DETAJE PËR KONTAKT TË KONTROLLORIT: Emri, adresa, posta elektronike, telefoni
DETAJE PËR KONTAKT PËR KONTROLLORË TË PËRBASHKËT: Emri, adresa, posta elektronike, telefoni
DETAJE PËR KONTAKT TË PËRFAQËSUESIT:* Emri, adresa, posta elektronike, telefoni
(*) Nëse është e aplikueshme DETAJE PËR KONTAKT TË OFICERIT PËR MBROJTJE TË TË DHP: Emri, adresa, posta elektronike, telefoni

Shënim: Raporti ndërmjet kontrollorit dhe përpunuesit dhe ndërmjet përpunuesit dhe çdo nënpërpunuesi, doemos duhet të bazohen në kontratë me shkrim për përmbushje të kërkesave për përpunim të të dhënave personale.

Përpunuesit duhet të ruajnë kopje të kontratave përkatëse me formularin e plotësuar.

Formulari për përpunuesin – Të dhënat bazë për aktivitetet për përpunim të të dhënave personale

Kategoria (lloji) i përpunimit që realizohet për kontrollorin lidhur me përpunimin, përfshirë edhe:	
– kategori të subjekteve të të dhënave personale	
– kategori të të dhënave personale	
A janë transferuar të dhënat në vendin e tretë ose te organizata ndërkombëtare?	
Në rast të transferimit të të dhënave personale: cilat masa mbrojtëse adekuate janë siguruar?	
Përshkrimi i përgjithshëm i masave teknike dhe organizative	
A përfshin përpunimi përdorim të nënpërpunuesit (ve)? Nëse po, shënoni detaje të plota dhe kopje të kontratave relevante.	

SHTOJCA 2 – PROPOZIM-DETAJE PËR HARTËZIM TË AKTIVITETEVE PËR PËRPUNIM TË TË DHËNAVE PERSONALE

II.1. Të dhënat dhe burimet e të dhënave

1. Cilat të dhëna personale ose kategori të të dhënave personale mblidhen dhe përdoren për këtë aktivitet për përpunim?	Shënoni me √ nëse është e aplikueshme	Kur, si dhe prej kujt janë marrë të dhënat personale? P.sh.: (subjekti i të dhënave personale) gjatë punësimit të personit gjatë përfshirjes në hulumtim...
Emri dhe mbiemri		
Datëlindja		
Adresa		
Numri i telefonit (privat/ zyrtar)		
E-mail (privat/zyrtar)		
Shtoni të dhëna plotësuese, nëse është e aplikueshme*		
2. A përfshijnë ose zbulojnë tërthorazi të dhënat që i mblidhni lidhur me aktivitetin, ndonjë prej kategorive të veçanta të të dhënave personale ("të dhëna të ndjeshme) në vijim?	Shënoni me √ nëse të dhënat mblidhen dhe shfrytëzohen rreptësisht për aktivitetin; Shënoni me √ dhe shtoni ("tërthorazi") nëse e dhëna është zbuluar tërthorazi (sqaro nëse është e domosdoshme)	Kur, si dhe prej kujt janë marrë të dhënat? P.sh.: (subjekt i të dhënave personale) - gjatë punësimit të personit - gjatë përfshirjes në hulumtim...
Origjina racore ose etnike		
Mendimet ose Përparësitë politike		
Besimi religjioz ose filozofik		

Anëtarësi në sindikatë		
Të dhënat gjenetike		
Të dhënat biometrike		
Të dhënat për shëndetin personal		
Informata për aktgjykime penale ose kundërvajtje		
3. Të dhëna tjera që kanë të bëjnë me përpunimin specifik	Shënoni me √ nëse është e aplikueshme	Kur, si dhe prej kujt janë marrë të dhënat personale? P.sh.: (subjekti i të dhënave personale) gjatë punësimit të personit gjatë përfshirjes së hulumtimit...
NUAQ		
Të dhënat për borxhe/kredi		
Të dhëna për të mitur		
4. Nëse është e njohur ose e përcaktuar: Sa gjatë ruhen të dhënat personale? Çfarë ndodh më pas?*		
* Cekni periudhën ose ngjarjen, p.sh., "7 vite" ose "Deri në 5 vjet pas ndërprerjes së punësimit". Sqaroni dhe çfarë ndodh me të dhënat, p.sh., fshirje/ shkatërrim ose nëse ato ruhen në formë të anonimizuar. Shënim: Nëse ekzistojnë periudha të ndryshme për ruajtje për të dhëna të ndryshme, ju lusim cekni.		

II.2. Zbulimi i të dhënave

5. Cilëve persona të tretë u zbulohen të dhënat e lartpërmendura? Dhe cilat qëllime Shënime: Kjo, gjithashtu, vlen edhe për të dhënat që bëhen të disponueshme, veçanërisht drejtpërdrejt, në formë elektronike Rizbulimet që përfshijnë transferime ndaj vendit të tretë	Personi i tretë marrë, vendi dhe shteti i themelimit	Qëllimi(et) e zbulimit
TË GJITHA TË DHËNAT E CEKURA NË II.1		
OSE: Të dhënat në vijim: (Kopjoji të dhënat nga 1 dhe 2 më lart)		
Nëse nevojitet, shtoni radhët plotësuese		

II.3. Baza juridike për përpunim

6. Baza juridike për përpunim të të dhënave	Shënoni bazën juridike relevante dhe jepni sqarim në kolonën në vijim, nëse është e aplikueshme	Sqarim
Subjekti i të dhënave personale ka dhënë pëlqim për përpunim		
Përpunimi është i domosdoshëm për raportin kontraktues ndërmjet organizatës dhe subjektit të të dhënave personale (ose me qëllim të ndërmarrjes së hapave të mëtutjeshme me kërkesë të subjektit të të dhënave personale para se të lidhet kontratë – p.sh., punësim)		

Përpunimi është i domosdoshëm për harmonizim me obligimin ligjor* për shembull, Ligji për marrëdhënie obligative – ju lutemi cekni ligjin në fjalë		
Përpunimi është i domosdoshëm që të mbrohen interesat thelbësore të subjektit të të dhënave personale ose të personit tjetër		
Përpunimi është i domosdoshëm për kryerjen e detyrës me interes publik* * Cekni burimin e detyrës (zakonisht ligjin nga i cili del)		
6.1. PËLQIM (detaje)		
Nëse të dhënat janë përpunuar në bazë të pëlqimit të subjekteve të të dhënave personale, si dhe kur është marrë ky pëlqim? Shënim: Nëse pëlqimi është dhënë në formë të letrës ose në formë elektronike, cekni kopje nga teksti përkatës		
Sa gjatë ruhet kjo dëshmi?		
A është përcaktuar mënyra në të cilën subjekti mund ta tërheqë pëlqimin?		

II.4. Informimi i subjekteve të të dhënave personale

[Shënim: Kjo informatë nuk është e detyrueshme, por është e dobishme gjatë vlerësimit dhe rishikimit të politikave të brendshme (interne) për mbrojtjen e të dhënave]

7. Informimi i subjekteve të të dhënave personale	Cekni Po/Jo (ose "nuk është e aplikueshme") Shënim: Nëse është relevante, mund, mund të cekni, "Është e dukshme në kontekstin" dhe/ose "Subjekti i të dhënave tashmë i posedon këto informata"	Sqaroni kur dhe si është bërë Ju lutemi jepni kopje të çfarëdo informatave, njoftimeve ose lidhjeve
Nëse subjektet e të dhënave personale janë informuar për përpunim? Dhe nëse përgjigja është vërtetuar, kur dhe si?		
A është organizata juaj kontrollori i përpunimit të të dhënave personale për aktivitet konkret?		
Nëse është e aplikueshme, a përmban informata detaje për përfaqësuesin tuaj në BE?		
A përmban informata detaje për kontakt të oficerit për mbrojtje të të dhënave personale		
A përmban informata qëllim kryesor të përpunimit		
A përmban informata qëllim të mëtutjeshëm për të cilin organizata juaj dëshiron (ose ndoshta është e interesuar) t'i përpunojë të dhënat		
A përmban informata a janë marrë të dhënat drejtpërdrejtë nga subjektet e të dhënave personale, cili është burimi dhe nëse ato përfshijnë informata të disponueshme publikisht (si për shembull, regjistra publike)?		

A i përmban informata pranuesit ose kategoritë e pranuesve të të dhënave personale?		
A përmban informata a (a do të) transferohen të dhënat në vendin jashtë BE-së/Hapësirës ekonomike evropiane (p.sh., në shërbime në "cloud" ku gjendet serveri në SHBA)? Shënim: Kjo, gjithashtu, vlen edhe për të dhënat që janë të disponueshme (veçanërisht drejtpërdrejt, online) për subjektet të cilët nuk janë pjesë e vendeve të BE-së/EEA-së.		
A përmban informata nëse të dhënat janë transferuar, cilat masa mbrojtëse janë paraparë, dhe ku mund të marrin kopje prej tyre subjektet e të dhënave personale? Shënim: Masat mbrojtëse mund të parashihen në kontratat për transferim të të dhënave personale ose përmes shifrave private ose vulave për privatësi.		
A përmban informata sa kohë ruhen të dhënat?		
A i përmban informata të drejtat e subjekteve të të dhënave personale të kërkojnë qasje, korrigjim ose fshirje të të dhënave personale; të kërkojnë të dhënat e tyre të mos jenë objekt i përpunimit të mëtutjeshëm, të negociojnë për përpunimin etj.		
A përmban informata të drejtën e subjekteve për të parashtruar ankesë në Agjencinë për Mbrojtjen e të Dhënave Personale?		

A përmban informata të dhëna nëse për të gjithë ose një pjesë e të dhënave që përpunohen në bazë të pëlqimit të marrë, janë informuar subjektet e të dhënave personale?		
A përmban informata nëse subjektet mund ta tërheqin pëlqimin e tyre në cilëndo kohë (dhe si ta bëjnë atë pa ndikuar kjo mbi ligjshmërinë e përpunimit paraprak)?		
8. Nëse subjektet e të dhënave personale nevojitet të jenë objekt i vendimmarrjes automatike ose profilizimit, nëse ato janë informuar për si në vijim;		Cekni një pasqyrë të shkurtër të logjikës së aplikuar gjatë vendimmarrjes automatike ose profilizimit.
Se do të aplikohet vendimmarrja ose profilizimi i tillë?		
Në përgjithësi, cila është "logjika" për profilizim?		
Çfarë rëndësie ka vendimmarrja automatike ose profilizimi dhe cilat janë pasojat nga mënyra e tillë e vendimmarrjes ose profilizimit?		

II.5. Transferimi ndërkufitar i të dhënave (transferimi i të dhënave në vendet e treta)

9. A transferohen të dhënat personale në vendin e tretë [nuk është BE/FEE] (ose sektor në vendin e tretë) ose në organizatën ndërkombëtare që nevojitet të sigurojë nivel "adekuat" të mbrojtjes?	Theksoni Po/Jo dhe vendin/et për të cilat bëhet fjalë. Nëse transferimi është vetëm për një pjesë, por jo për të gjitha të dhënat, theksoni për secilën kategori të të dhënave.	Shpjegoni qëllimin e transferimit, p.sh.: si një pjesë e aktiviteteve të organizatës suaj (p.sh.: kur përdorni softuer të bazuar në re), ose si një pjesë e obligimit për zbulimin e të dhënave te personi i tretë (ju lutemi theksoni atë palë)
TË GJITHA TË DHËNAT TË THEKSUARA NË II.1.		
Nëse është e nevojshme, shtoni rreshta shtesë		

10. A janë transferuar disa nga të dhënat në vendet e treta (nuk janë BE/ Fusha Ekonomike Evropiane) ose organizatën ndërkombëtare që nuk ka për obligim të ofrojë nivel "adekuat" të mbrojtjes?	Theksoni Po/Jo dhe vendin/et në fjalë. Nëse transferimi është vetëm për një pjesë, por jo për të gjitha të dhënat, theksoni për secilën kategori të të dhënave.	Shpjegoni qëllimin e transferimit, p.sh.: si një pjesë e aktiviteteve të organizatës suaj (p.sh.: kur përdorni softuer të bazuar në re), ose si një pjesë e obligimit për zbulimin e të dhënave te personi i tretë (theksoni palën e tretë)	Çfarë mbrojtjeje ose përjashtimi po përdorni për të mbështetur këtë transferim? *Shënim: Siguroni kopje të çdo dokumenti relevant
Shënim: Nëse të dhënat transferohen për qëllime të ndryshme të marrësve të ndryshëm në vende të ndryshme, ju lutemi përgjigjuni pyetjeve veçmas për çdo transferim.			

TË GJITHA TË DHËNAT TË THEKSUARA NË II.1.			
OSE: Të dhënat si në vijim: **(Kopjoni të dhënat nga 1 dhe 2, më sipër)**			
Nëse është e nevojshme, shtoni rreshta shtesë			
SHËNIM: Sipas LMDHP-së, transferimet në vendet që nuk ishin të detyrueshme të ofrojnë "nivel adekuat" të mbrojtjes mund të ndodhin vetëm nëse ekzistojnë "masa mbrojtëse përkatëse", siç theksohet në kolonën e majtë, më poshtë, ose nëse zbatohet lëshimi, siç theksohet në kolonën e djathtë			

Masat mbrojtëse sipas LMDHP-së: 1. Instrumenti ndërkombëtar ndërmjet organeve publike; 2. Rregullat korporative detyruese; 3. Klauzolat standarde të miratuara për transferimin e të dhënave; 6. Klauzola të miratuara ad hok.	Përjashtime, nëse mbrojtjet adekuate nuk janë të disponueshme: 7. Pëlqimi; 8. Kontrata ndërmjet kontrollorit dhe subjektit të të dhënave personale; 9. Kontrata ndërmjet kontrollorit dhe personit të tretë; 10. E domosdoshme për arsye të rëndësishme me interes publik; 11. Të nevojshme për pretendimet juridike; 12. E domosdoshme për të mbrojtur interesat thelbësore të subjektit të të dhënave personale ose të tjera; 13. Transferimi bëhet nga regjistri i disponueshëm për publikun.
A ka rregulla për të vepruar në bazë të ndonjë aktgjykimi të gjykatës ose tribunalit dhe të ndonjë vendimi të organit administrativ të vendit të tretë që mund t'i shërbejë kontrollorit ose çdo përpunuesi dhe që kërkon që kontrollori ose përpunuesi të kryejë transferim ose zbulim të të dhënave personale? (nuk është e detyrueshme, por rekomandohet për të evidentuar, të plotësohet)	Theksoni Po/Jo dhe nëse po, ju lutemi jepni kopje të udhëzimeve
Shënim: Theksoni Po/Jo dhe nëse po, ju lutemi jepni kopje të udhëzimeve	Ofroni detaje:
A ruhen të dhënat personale të theksuara në II.1. në letër ose në formë elektronike?	
Ku (fizikisht) ruhen të dhënat? (Në zyra? Në serverët e kontrollorit? Në serverët e organizatës shoqëruese? Në serverët e palëve të treta (p.sh.: ofruesi i shërbimeve në re)?	

Çfarë masash zbatohen për të mbrojtur nga qasja e paautorizuar në hapësirën fizike ku të dhënat ruhen / janë në dispozicion? A ka politikë të sigurisë së të dhënave që e rregullon këtë? (Nëse ka, ju lutemi ofroni kopje)	
Çfarë hardueri përdoret në përpunimin e të dhënave personale? Kush është përgjegjës për menaxhimin dhe sigurinë e këtij hardueri?	
A ruhet (ndonjë prej) të dhënave në media/pajisje portative? Në pronësinë e kujt janë mediat/pajisjet?	
A mund të përdorë ndonjë nga njerëzit me qasje në të dhënat pajisje personale për të hyrë ose për të përpunuar të dhënat? Nëse po, a ka politikë për të mbrojtur përdorimin e pajisjeve të veta? Nevojitet të ofroni kopje të politikës.	
A i nënshtrohen detyrimit të konfidencialitetit të gjithë personat e autorizuar për të hyrë në të dhënat personale (qoftë me ligj ose një sërë normash profesionale ose në përputhje me detyrimet kontraktuese)? Ju lutemi theksoni detaje ose kopje nga të gjitha klauzolet juridike ose kontraktuese relevante.	
Çfarë softuerësh/aplikacionesh përdoren për përpunimin e të dhënave? (p.sh.: pakoja për desktop e "Majkrosoft Ofis", aplikacioni i menaxhuar nga qendra, shërbimi në "re", etj.)	

A menaxhohet ky softuer në nivel lokal apo qendror? Nëse përpunimi është qendror, kush është entiteti qendror? Nëse nuk jeni ju, a ka marrëdhënie formale midis atij subjekti dhe organizatës suaj në lidhje me përdorimin e softuerit? Ju lutemi theksoni kopje të këtij dokumenti.	
A është softueri i bazuar në "re"? Nëse po, kush është ofruesi i shërbimeve dhe ku është i bazuar ligjërisht ai provajder? Ku janë të vendosur fizikisht serverët? A janë të kriptuar të dhënat në "re"? Si (përkatësisht duke përdorur çfarë teknologjie të enkriptimit)? Ju lutemi jepni kopje të kontratës mbi bazën e së cilës kryhet ky përpunim.	
Kush është përgjegjës (respektivisht kush është "administratori") i këtij softueri? (Ju? Dikush tjetër brenda organizatës suaj? Dikush në subjektin me të cilin jeni i lidhur? Pala e tretë?)	
A transferohen të dhënat në çdo kohë/në çdo rrethanë në mënyrë elektronike në media, sistem ose pajisje tjetër?	
Nëse transferohen në mënyrë elektronike, a është bërë kjo: - përmes internetit? Nëse po, a ishin të enkriptuar të dhënat? Në çfarë mënyre (respektivisht, duke përdorur çfarë teknologjie të enkriptimit)? - me ndihmën e FTP-së? Si sigurohet kjo? - me ndihmën e VPN-së? Si sigurohet kjo? - tjetër (theksoni)	

SHTOJCA 3: QASJA E MIRATUAR NGA ENISA (AGJENCIA EVROPIANE PËR SIGURINË KIBERNETIKE) E CILA BAZOHET NË STANDARDIN E PRANUAR NDËRKOMBËTARISHT ISO 27005: "KËRCËNIMET I KEQPËRDORIN DOBËSITË E MJETEVE QË ÇON NË SHKAKTIMIN E DËMIT TË ORGANIZATËS";

Source: ENISA Threat Landscape Report 2016, Figure 4: The elements of risk and their relationshipsaccording to ISO 15408:2005, https://www.enisa.europa.eu/publications/enisa-threat-landscapereport-2016. See also its 2017 report,https://www.enisa.europa.eu/publications/enisa-threatlandscape-report-2017.

Mjetet (vulnerabiliteti, kontrollet), kërcënimi (profili i agjentit për kërcënim, probabiliteti) dhe ndikimi.

Elementet e rrezikut dhe marrëdhëniet e tyre mund të paraqiten si më poshtë:

Përkufizimi i niveleve të ndryshme të ndikimit mund të grupohen në katër nivele, si në vijim:

Niveli i ndikimit	Përshkrimi
I ulët	Subjektet mund të ndeshen me disa shqetësime të vogla, të cilat do të tejkalohen pa problem (koha e kaluar për rishënimin e informacioneve, nervozet, irritimet, etj.).
I mesëm	Subjektet mund të ndeshen me shqetësime të rëndësishme, të cilat do të jenë në gjendje t'i tejkalojnë pavarësisht disa vështirësive (shpenzime shtesë, mohimi i qasjes në shërbimet e biznesit, frika, mungesa e mirëkuptimit, stresi, sëmundjet e vogla fizike, etj.).
I lartë	Subjektet mund të ndeshen me pasoja të rëndësishme që duhet të jenë në gjendje t'i tejkalojnë edhe me vështirësi serioze (përvetësimi i gabuar i mjeteve, futja në listën e zezë nga institucionet financiare, dëmi material, humbja e punës, ftesa, përkeqësimi i shëndetit, etj.).
Shumë i lartë	Subjektet që mund të ndeshen me pasoja të rëndësishme, madje edhe të pakthyeshme që mund të mos tejkalohen (paaftësia për të punuar, sëmundja afatgjate psikologjike ose fizike, vdekja, etj.).

Për çdo fushë të vlerësimit, parashtrohen pesë pyetje, për të cilat të paktën një përgjigje pozitive tregon rrezikun, siç theksohet në tabelë.

Vlerësuesi i rrezikut të sigurisë, nga këto përgjigje, mund të përcaktojë probabilitetin e shfaqjes së kërcënimit. Ky rezultat më pas mund të kombinohet me vlerësimin e ndikimit për të arritur në rrezikun e përgjithshëm për aktivitetin konkret të përpunimit të të dhënave personale.

KATËR FUSHAT KRYESORE TË VLERËSIMIT PËR SA I PËRKET SIGURISË SË TË DHËNAVE:

Rrjeti dhe resurset teknike	Proceset dhe procedurat	Palët dhe personat e përfshirë	Siguria dhe shkelja
1. A kryhet përmes internetit një pjesë e përpunimit të të dhënave personale?	6. A janë rolet dhe përgjegjësitë në lidhje me përpunimin e të dhënave personale të paqarta, përkatësisht pamjaftueshëm të përkufizuara qartë?	11. Nëse përpunimi i të dhënave personale kryhet nga një numër i pacaktuar punonjësish?	16. A konsideroni se industria juaj është e ndjeshme ndaj sulmeve në hapësirën digjitale?
2. A është e mundur të sigurohet qasja në sistemin e brendshëm për përpunimin e të dhënave personale përmes internetit (p.sh.: për përdorues të caktuar ose grupe përdoruesish)?	7. Nëse përdorimi i rrjetit, sistemit dhe resurseve fizike brenda organizatës është i paqartë ose nuk është i përkufizuar qartë?	12. A kryhet ndonjë pjesë e aktiviteteve të përpunimit të të dhënave personale nga realizuesi/ pala e tretë (përpunuesi i të dhënave)?	17. A ka pësuar organizata juaj sulm në hapësirën digjitale ose ndonjë lloj tjetër të incidentit/shkeljes së sigurisë në dy vitet e fundit?
3. A është sistemi i përpunimit të të dhënave personale i ndërlidhur me sistemin ose shërbimin tjetër të jashtëm ose të brendshëm të TI-së që i përket organizatës suaj?	8. A lejohen punonjësit të sjellin dhe përdorin pajisjet e tyre portative për t'u lidhur me sistemin e përpunimit të të dhënave personale?	13. Nëse detyrimet e palëve/ personave të përfshirë në përpunimin e të dhënave personale janë të paqarta ose të theksuara në mënyrë të paqartë?	18. A keni marrë ndonjë njoftim dhe/ose ankesë në lidhje me sigurinë e sistemit të TI-së (që përdoret për përpunimin e të dhënave personale), në vitin e fundit?
4. A mund të hyjnë lehtësisht personat e paautorizuar në mjedisin ku përpunohen të dhënat personale?	9. A lejohen punonjësit të transferojnë, mbledhin ose në mënyrë tjetër të transmetojnë të dhëna personale jashtë ambienteve të organizatës?	14. A nuk janë të njoftuar punonjësit që janë të përfshirë në përpunimin e të dhënave personale me çështjet që lidhen me sigurinë e informacioneve të të dhënave?	19. A përfshin evidenca e aktiviteteve të përpunimit vëllim të madh subjektesh dhe/ ose të dhënash personale?

5. Nëse sistemi i përpunimit të të dhënave personale është dizajnuar, zbatuar ose mirëmbajtur pa ndjekur praktikat më të mira relevante?	10. A mund të kryhet përpunimi i të dhënave personale pa gjurmë përkatëse të revizorit (logot)?	15. A e neglizhojnë personat/palët e përfshirë në përpunimin e të dhënave procedurën e ruajtjes së sigurt dhe/ose shkatërrimit të të dhënave personale?	20. A ka praktika më të mira të sigurisë që janë specifike për sektorin tuaj të biznesit që nuk janë zbatuar në mënyrë adekuate?

PROBABILITETI I SHFAQJES SË KËRCËNIMIT (1):

Fusha e vlerësimit	Numri "PO" përgjigju pyetjeve më poshtë	Niveli	Pikët
Rrjeti dhe resurset teknike	0-1	I ulët	1
	2-3	I mesëm	2
	4-5	I lartë	3
Proceset dhe procedurat	0-1	I ulët	1
	2-3	I mesëm	2
	4-5	I lartë	3
Palët dhe personat e përfshirë	0-1	I ulët	1
	2-3	I mesëm	2
	4-5	I lartë	3
Siguria dhe shkelja	0-1	I ulët	1
	2-3	I mesëm	2
	4-5	I lartë	3

Rezultatet e mësipërme janë shënuar në tabelën përmbledhëse të mëposhtme:

PROBABILITETI I SHFAQJES SË KËRCËNIMIT (2):

Shuma e përgjithshme	Niveli për probabilitetin e shfaqjes së kërcënimeve
4-5	I ulët
6-8	I mesëm
9-12	I lartë

Në fund, këto rezultate më pas mund të kombinohen me rezultatet e "Nivelit të ndikimit" për të treguar rrezikun e përgjithshëm, si më poshtë:

VLERËSIMI I PLOTË I RREZIKUT

rreziku = probabiliteti x ndikimi

Probabiliteti	**Matrica e rrezikut**			
L (i lartë)	**U**	**M**	**L**	**SHL**
M (i mesëm)	**U**	**M**	**L**	**SHL**
U (i ulët)	**U**	**N**	**M**	**L**
Ndikimi	**U** (i ulët)	**M** (i mesëm)	**L** (i lartë)	**SHL** (shumë i lartë)

SHTOJCA 4 – SHEMBUJ TË SHKELJES SË SIGURISË SË TË DHËNAVE PERSONALE DHE KË DUHET NJOFTUAR (NGA UDHËZIMET E WP29)

Shembull	Njoftoni autoritetin mbikëqyrës?	Njoftoni subjektet e të dhënave personale?	Shënime / rekomandime
i. Kontrollori ka ruajtur kopje rezervë të arkivit të të dhënave personale, e cila është e enkriptuar me çelës. Çelësi u vodh gjatë kohës së qasjes së paautorizuar.	Jo	Jo	Për sa kohë që të dhënat janë të enkriptuara dhe ka kopje rezervë të të dhënave të ruajtura me çelës unik që nuk është kompromentuar dhe të dhënat mund të rinovohen brenda një periudhe të pranueshme, kjo nuk mund të trajtohet si shkelje që duhet të paraqitet. Megjithatë, nëse çelësi unik kompromentohet më vonë, nevojitet njoftimi.

ii. Kontrollori mban servis online. Si rezultat i sulmit kibernetik ndaj atij servisi, të dhënat personale u vodhën. Kontrollori ka klientë në vendet anëtare të BE-së.	Po, paraqitni në AMDHP, nëse ka probabilitet për pasoja në të dhënat personale të subjekteve që përdorin atë servis.	Po, paraqitni te subjektet e interesuara, në varësi të natyrës së të dhënave personale dhe nëse probabiliteti dhe serioziteti i pasojave për subjektet është i lartë.	
iii. Ndërprerja e shkurtër e rrymës që zgjat disa minuta, gjatë së cilës klientët nuk mund të kenë qasje në të dhënat e tyre	Jo	Jo	Ky nuk është njoftim për shkeljen e sigurisë së të dhënave personale, por është incident i sigurisë që ai duhet të regjistrohet në evidencën përkatëse të incidenteve.
iv. Kontrollori vuan nga sulmi ransomware që rezulton në enkriptimin e të gjitha të dhënave. Nuk ka kopje rezervë të disponueshme dhe të dhënat nuk mund të rikthehen. Gjatë hetimit, bëhet e qartë se funksionaliteti i softuerit blerës (ransomware's) ishte t'i bllokonte (kriptonte) të dhënat dhe se nuk u konstatua asnjë softuer tjetër me qëllim të keq që të ishte i pranishëm në sistem.	Po, paraqitni në AMDHP, nëse ka probabilitet për pasojat, për subjektet e të dhënave personale duke pasur parasysh se bëhet fjalë për humbjen e disponueshmërisë së tyre.	Po, paraqitni te subjektet e të dhënave personale, në varësi të natyrës së të dhënave personale të prekura dhe tregoni për efektin e mundshëm të mungesës së disponueshmërisë së të dhënave, si dhe të gjitha pasojave të tjera të ngjashme.	Nëse kishte kopje rezervë të disponueshme dhe të dhënat mund të rinovohen në kohë, kjo nuk duhet t'i paraqitet AMDHP-së ose subjekteve të të dhënave personale, pasi nuk ka ndodhur humbja e përhershme e konfidencialitetit. Megjithatë, nëse AMDHP-ja merr informacion për incidentin në mënyrë tjetër, mund të kryejë hetim për të vlerësuar harmonizimin me kërkesat e sigurisë.

v. Të dhënat personale të një numri të madh studentësh janë dërguar gabimisht në postën e gabuar elektronike që përmban 1000+ marrës.	Po, paraqitni në AMDHP.	Po, njoftoni subjektet e të dhënave personale, në varësi të fushëveprimit dhe llojit të të dhënave personale që përfshihen, si dhe nga serioziteti i pasojave të mundshme.	

SHTOJCA 5 – LISTA KONTROLLUESE PËR OFICERIN PËR MBROJTJEN E TË DHËNAVE PERSONALE NË LIDHJE ME HARMONIZIMIN E PUNËS SË KONTROLLORIT ME LIGJIN PËR MBROJTJEN E TË DHËNAVE PERSONALE DHE AKTET NËNLIGJORE PËRKATËSE NË FUSHËN E MBROJTJES SË TË DHËNAVE PERSONALE

Emri i kontrolluesit: _____

Oficeri për mbrojtjen e të dhënave personale (emri dhe mbiemri, posta elektronike, etj.): _____

Viti: _____

(Rekomandohet që kjo listë kontrolluese të plotësohet në nivel vjetor, në fund të çdo viti kalendarik, nga oficeri për mbrojtjen e të dhënave personale, për të ndjekur përmbushjen e detyrimeve që rrjedhin nga rregullat për mbrojtjen e të dhënave personale)

Vërejtje: Lista e pyetjeve mund të shërbejë si orientim për të marrë një pasqyrë të harmonizimit momental të kontrolluesit me rregullativën relevante në fushën e mbrojtjes së të dhënave personale.

1. A ka emëruar kontrollori oficer për mbrojtjen e të dhënave personale, me akt juridik intern përkatës (vendim, aktvendim, etj.) me të cilin është emëruar në këtë pozitë dhe i cili i posedon kualifikimet e nevojshme në përputhje me LMDHP-në?

a) PO

b) JO

c) Shënim: _____

2. A i përgjigjet oficeri drejtpërdrejt udhëheqësisë së kontrollorit?

a) PO

b) JO

c) Shënim: _____

3. A ka oficeri komunikim të rregullt me udhëheqësin e kontrollorit?

a) PO

b) JO

c) Shënim: _____

4. A ka oficeri në dispozicion resurset e nevojshme për të ushtruar funksionin e tij (hapësirën e punës, pajisjet, qasjen e papenguar dhe të drejtpërdrejtë në dokumentet e domosdoshme, etj.)?

a) PO

b) JO

c) Shënim: _____

5. A kryen oficeri për mbrojtjen e të dhënave personale edhe detyra të tjera pune që mund të çojnë në konflikt të mundshëm të interesave?

a) PO

b) JO

c) Shënim: _____

6. A merr pjesë oficeri në trajnimet e organizuara dhe të zbatuara nga Agjencia për Mbrojtjen e të Dhënave Personale, si dhe në edukimet e tjera profesionale?

a) PO

b) JO

c) Shënim: _____

7. A i ka publikuar kontrolluesi të dhënat e kontaktit të oficerit për mbrojtjen e të dhënave personale dhe ka dorëzuar njoftim në Agjencinë për Mbrojtjen e të Dhënave Personale?

a) PO

b) JO

c) Shënim: _____

8. A ka kontrolluesi akte interne për mbrojtjen e të dhënave personale? (p.sh., Politika / Deklarata e Privatësisë, Politika për përdorimin e biskotave, Rregullorja për mënyrën e kryerjes së video-mbikëqyrjes, Procedura për të drejtat e subjekteve të të dhënave personale, etj.)

a) PO

b) JO

c) Shënim: _____

9. A përgatit kontrolluesi vlerësim të ndikimit të aktiviteteve të planifikuara të përpunimit të të dhënave në mbrojtjen e të dhënave personale (Data Protection Impact Assessment)?

a) PO

b) JO

c) Shënim: _____

10. Nëse kontrollor për aktivitetet përkatëse për përpunimin e të dhënave personale ka miratuar akte interne me të cilat përcaktohet plani dhe rregullohen në mënyrë përkatëse masat teknike dhe organizative për sigurimin e fshehtësisë dhe mbrojtjes së përpunimit të të dhënave personale; përcaktimin e detyrimeve dhe përgjegjësive të administratorit të sistemit të informacioneve dhe të personave të autorizuar gjatë përdorimit të dokumenteve dhe pajisjeve informative-komunikuese, rregullimin e procedurës së paraqitjes, reagimit dhe korrigjimit të incidenteve; përcaktimin e procedurës për mënyrën e bërjes së kopjes së sigurisë, arkivimin dhe ruajtjen, si dhe për rikthimin e të dhënave të ruajtura personale; si dhe procedurën për mënyrën e shkatërrimit të dokumenteve, si dhe për mënyrën e shkatërrimit, fshirjes dhe pastrimit të mediave, etj.)

a) PO

b) JO

c) Shënim: _____

11. A i zbaton masat e përcaktuara teknike dhe organizative kontrollori gjatë aktiviteteve për përpunimin e të dhënave personale në kuadër të proceseve të biznesit?

(Vërejtje: Të theksohet individualisht për çdo aktivitet të përpunimit të të dhënave personale)

a) PO

b) JO

c) Shënim: _____

12. A janë identifikuar rreziqet për sa i përket fshehtësisë dhe mbrojtjes së të dhënave personale?

a) PO

b) JO

c) Shënim: _____

13. A është vendosur dhe a përditësohet rregullisht evidenca (Regjistri) e aktiviteteve të përpunimit të të dhënave personale? A përmban evidenca: emërtimin e aktivitetit të përpunimit, qëllimin e përpunimit, bazën juridike për përpunimin e të dhënave personale, afatet e fshirjes, nëse të dhënat personale transferohen në vendet e treta, etj.)

a) PO

b) JO

c) Shënim: _____

14. A ka regjistruar kontrollori shkelje të sigurisë për mbrojtjen e të dhënave personale dhe a është evidentuar shkelja në mënyrë përkatëse, duke përfshirë edhe shkaqet e shkeljes, pasojat dhe masat e ndërmarra për ta hequr atë?

a) PO

b) JO

c) Shënim: _____

15. A ka pasur shkelje te kontrollori që mund të çojë në rrezik për të drejtat dhe liritë e personave fizikë dhe a është njoftuar Agjencia për Mbrojtjen e të Dhënave Personale për këtë?

a) PO

b) JO

c) Shënim: _____

16. A transferon kontrollori të dhëna për individët në vende të tjera ose organizata ndërkombëtare, në përputhje me ligjin?

a) PO (të theksohen se cilat të dhëna, ku, kujt, baza juridike për transferimin)

b) JO

c) Shënim: _____

17. A janë lidhur kontratat e përpunimit të të dhënave personale ndërmjet kontrollori dhe përpunuesit me rregullat dhe procedurat e detajuara për të siguruar nivel adekuat të mbrojtjes së të dhënave personale gjatë përpunimit të tyre? (klauzolat standarde)

a) PO

b) JO

c) Shënim: _____

18. A përpunon kontrollori kategori të veçantë të dhënash personale (të dhëna që zbulojnë origjinën racore ose etnike, mendimin politik, besimin fetar ose filozofik ose anëtarësimin në sindikatë, si dhe të dhënat gjenetike, të dhënat biometrike, për qëllimet e identifikimit unik, të dhënat e gjendjes shëndetësore ose të dhënat rreth jetës seksuale ose orientimit seksual të personit fizik)? Dhe a konsultohet oficeri për këtë?

a) PO (të theksohen se cilat të dhëna, ku, kujt, baza juridike për transferimin)

b) JO

c) Shënim: _____

19. A i përpunon kontrollori të dhënat mbi aktgjykimet dhe sanksionet penale dhe nëse për përpunimin e këtyre të dhënave personale zbaton masa të veçanta për mbrojtjen e të drejtave dhe lirive të individëve të cilëve u referohen këto të dhëna personale?

a) PO (të theksohet në përbërjen e institucionit në cilin aktivitet për përpunimin e të dhënave personale përpunohen këto të dhëna, baza juridike dhe për çfarë qëllimi)

b) JO

c) Shënim: _____

20. A ka kontrollori përpunues që përpunon të dhëna personale në emër të tij dhe marrëdhënia me ta rregullohet nga kontrata ose akti tjetër juridikisht i obligueshëm?

a) PO (të theksohet se cilat aktivitete të përpunimit të të dhënave personale i janë dhënë përpunuesit/ve dhe me cilin akt rregullohet kjo marrëdhënie)

b) JO

c) Shënim: _____

21. A zbulon kontrollori të dhënat personale të marrësve (personi fizik ose juridik, përkatësisht organi i pushtetit shtetëror?

a) PO (të theksohet se cilat të dhëna, identiteti i marrësit, baza juridike dhe qëllimi i zbulimit të të dhënave personale)

b) JO

c) Shënim: _____

22. Nëse bëhet fjalë për kontrollori të përbashkët, a ka qëllim dhe mënyrë të përpunimit të të dhënave personale dhe nëse për atë përpunim kanë kontratë të ndërsjellë?

a) PO (të theksohet në kuadër të cilit aktivitet, kush është pronar i procesit të biznesit dhe me cilën kontratë rregullohet)

b) JO

c) Shënim: _____

23. A përgatit oficeri plan për mbajtjen e edukimit (trajnimit) për mbrojtjen e të dhënave personale, të përshtatur me nevojat e punonjësve të institucionit (themelore, të avancuara, të specializuara, etj.)

a) PO

b) JO

c) Shënim: _____

24. A organizon dhe realizon oficeri komunikim të rregullt me të gjithë punonjësit, palët e treta me të cilët bashkëpunon etj., për të rritur ndërgjegjësimin për mbrojtjen e të dhënave personale?

a) PO

b) JO

c) Shënim: _____

25. A ka ndonjë procedurë të përcaktuar me pëlqimin e së cilës oficeri është i përfshirë me mendimin e tij profesional në përgatitjen dhe zhvillimin e produkteve, shërbimeve dhe sistemeve të reja të TI-së?

a) PO

b) JO

c) Shënim: _____

26. A është oficeri i përfshirë me mendim në lidhje me sigurimin e pëlqimit të subjekteve të të dhënave personale, për përpunimin e të dhënave të tyre personale?

a) PO

b) JO

c) Shënim: _____

27. A konsultohet oficeri gjatë përpunimit të kategorive të veçanta të të dhënave personale?

a) PO

b) JO

c) Shënim: _____

28. A kryen oficeri revizione / kontrolle / inspektime të respektimit të rregullave për mbrojtjen e të dhënave personale?

a) PO

b) JO

c) Shënim: _____

29. A ka plan vjetor për kryerjen e revizioneve / kontrolleve / inspektimeve të miratuar nga oficeri dhe nëse është e aplikueshme, a është zbatuar për vitin e kaluar?

a) PO

b) JO

c) Shënim: _____

30. A ka vepruar kontrollori sipas konstatimeve dhe rekomandimeve, brenda afateve të dhëna për veprim? (të theksohet se çfarë akoma nuk është mbyllur)

a) PO

b) JO

c) Shënim: _____

31. A është vepruar sipas konstatimeve të kontrolleve të jashtme? (të theksohet se çfarë akoma nuk është mbyllur)

a) PO

b) JO

c) Shënim: _____

32. A kryhen kontrolle periodike në përputhje me dokumentacionin për masat teknike dhe organizative?

Vërejtje: Është e nevojshme t'i përgjigjeni secilit prej opsioneve të mësipërme veç e veç:

a) PO

b) JO

c) Shënim: _____

33. A ka vepruar kontrollori sipas konstatimeve të raportit të kontrollit periodik dhe ka njoftuar oficerin dhe personat përgjegjës të kontrollorit?

a) PO

b) JO

c) Shënim: _____

34. A është kryer mbikëqyrja inspektuese te kontrollori nga Agjencia për Mbrojtjen e të Dhënave Personale? A janë konstatuar shkelje ose parregullsi me aktvendim, përkatësisht a janë dhënë rekomandime të caktuara? Nëse po, a është vepruar sipas tyre?

a) PO

b) JO

c) Shënim: _____

35. Nëse në rast të transferimit të të dhënave personale jashtë vendeve të BE-së dhe FEE-së, oficeri ndërmerr aktivitete për inicimin e procedurës për marrjen e miratimit përkatës për transferimin nga Agjencia për Mbrojtjen e të Dhënave Personale?

a) PO

b) JO

c) Shënim: _____

36. A kanë marrë punonjësit autorizim për përpunimin e të dhënave personale?

a) PO

b) JO

c) Shënim: _____

37. A kanë nënshkruar punonjësit deklaratë për fshehtësinë dhe mbrojtjen e të dhënave personale?

a) PO

b) JO

c) Shënim: _____

38. A ka vendosur kontrollori dhe a e përditëson rregullisht evidencën e personave të autorizuar për përpunimin e të dhënave personale?

a) PO

b) JO

c) Shënim: _____

39. A janë punonjësit të njoftuar me dokumentacionin për masat teknike dhe organizative dhe a është në dispozicion të tyre?

a) PO

b) JO

c) Shënim: _____

40. A dorëzohen raportet e parregullsive nga punonjësit te oficeri?

a) PO

b) JO

c) Shënim: _____

41. A e ka njoftuar kontrollori Agjencinë për përpunimin me rrezik të lartë (të të dhënave personale)?

a) PO

b) JO

c) Shënim: _____

42. A informon kontrollori në rast të shkeljes së sigurisë, përkatësisht shkeljes së të dhënave personale?

a) PO

b) JO

c) Shënim: _____

43. A kanë subjektet e të dhënave personale të drejtën e qasjes në informacionet në lidhje me përpunimin përkatës të të dhënave të tyre personale dhe nëse këto informacione janë lehtësisht të qasshme për subjektet e interesuara?

a) PO

b) JO

c) Shënim: _____

44. A është përgatitur formulari i kërkesës për ushtrimin e të drejtave të subjekteve të të dhënave personale dhe procedura se si subjektet e të dhënave personale mund t'i ushtrojnë të drejtat e tyre?

a) PO

b) JO

c) Shënim: _____

45. A janë punonjësit të njoftuar me aktet interne se si subjektet e të dhënave personale mund të kenë qasje në të dhënat e tyre personale?

a) PO

b) JO

c) Shënim: _____

46. A është paraparë procedura që siguron që kundërshtimet dhe shënimet në lidhje me përpunimin e të dhënave personale do të shqyrtohen pa anulim?

a) PO

b) JO

c) Shënim: _____

45. A është paraparë procedura që siguron që në rast se kryhet marketingu i drejtpërdrejtë, subjektet e të dhënave personale informohen për të drejtat e tyre?

a) PO

b) JO

c) Shënim: _____

K O M E N T E

_____

_____

_____

_____

SHTOJCA 6 – ÇEKING-LISTA PËR ZBATIMIN E MASAVE TEKNIKE DHE ORGANIZATIVE NË PËRPUTHJE ME RREGULLOREN E SIGURISË DHE PRAKTIKAT MË TË MIRA TË BE-SË

Lista e masave		Masa	
1.	Rritja e ndërgjegjësimit të përdoruesve	Informimi dhe ndërgjegjësimi i individëve për mënyrën e menaxhimit të të dhënave	☐
2.	Autentifikimi	Përkufizimi i identifikuesit unik (login) për çdo përdorues	☐
		Miratimi i politikës për fjalëkalimet e përdoruesve sipas rekomandimeve të AMDHP-së	☐
		Ndryshimi i detyrueshëm (i detyruar) i fjalëkalimit për çdo përdorues kur e rivendos atë.	☐
		Kufizimi i numrit të përpjekjeve të dështuara për hyrjen e përdoruesve	☐
3.	Menaxhimi i qasjeve	Përkufizimi i profileve	☐
		Heqja e privilegjeve të vjetruara të përdoruesve për qasje	☐
		Kryerja e kontrollit (revizionit) vjetor të qasjeve dhe privilegjeve	☐
4.	Logimi i qasjeve dhe menaxhimi i incidenteve	Zbatimi i sistemit për logim (logging)	☐
		Informimi i përdoruesve për zbatimin e sistemit për logim	☐
		Mbrojtja e pajisjeve të përdorura për logim dhe vetë logot	☐
		Zbatimi i procedurave të njoftimit në rast të cenimit të sigurisë së të dhënave personale	☐
5.	Siguria e stacioneve të punës	Përcaktimi i procedurës për mbylljen automatike të stacioneve të punës pasi të ketë kaluar periudha	☐
		Përdorimi i përditësimit të rregullt të antivirusit	☐
		Instalimi i "fajrvol" (firewall)	☐
		Marrja e pëlqimit nga përdoruesit gjatë ndërhyrjes në stacionin e tyre të punës	☐

6.	Siguria e përpunimit të të dhënave personale në pajisjet portative (celulare)	Përcaktimi i mekanizmave të enkriptimit për pajisjet portative (celulare)	☐
		Zbatimi i kopjeve rezervë dhe sinkronizimeve të rregullta	☐
		Përcaktimi i masës për zhbllokimin e telefonave inteligjentë (fjalëkalim, pin, etj.)	☐
7.	Mbrojtja e rrjetit të brendshëm	Kufizimi i komunikacionit të rrjetit, por i domosdoshëm vetëm për të qenë aktiv	☐
		Siguroni qasje në distancë përmes VPN-së	☐
		Zbatimi i protokollit WPA2 ose WPA2-PSK për rrjetet Wi-Fi	☐
8.	Sigurimi i serverëve	Lejimi i qasjes te mjetet dhe interfejsi i administratorit vetëm për personat e kualifikuar	☐
		Instalimi i përditësimeve kryesore pa anulim	☐
		Sigurimi i disponueshmërisë në të dhënat	☐
9.	Sigurimi i faqes së internetit / faqeve të internetit	Përdorimi i Protokollit TLS dhe kontrollimi i zbatimit të tij	☐
		Kontrollimi i fjalëkalimeve dhe identifikuesve se nuk transferohen përmes URL-së	☐
		Kontrollimi se ajo që kërkohet që përdoruesit t'i shënojnë i përmbush pritshmëritë e tyre	☐
		Futja e banerit për pëlqimin për përdorimin e biskotave për ata që nuk janë të domosdoshëm për të përdorur shërbimin	☐
10.	Sigurimi i vazhdimësisë	Kryerja e kopjeve të rregullta të sigurisë	☐
		Mbajtja e mediave ku kopja e sigurisë është në vend të sigurt	☐
		Zbatimi i masave të sigurisë për transferimin e kopjeve të sigurisë	☐
		Zbatimi dhe testimi i rregullt i planit të vazhdimësisë në punën	☐

11.	Arkivimi i sigurt	Zbatimi i metodave të caktuara për qasjen në të dhënat e arkivuara	☐
		Shkatërrimi i sigurt i arkivave të vjetruara	☐
12.	Mbikëqyrja e mirëmbajtjes dhe shkatërrimit të të dhënave	Mbajtja e evidencës së mirëmbajtjes në ndonjë lloj regjistri	☐
		Duke pasur person përgjegjës nga organizata që të mbikëqyrë punën e palëve të treta	☐
		Fshirja e të dhënave nga të gjithë harduerët përpara se të shkatërrohen	☐
13.	Menaxhimi i përpunuesve	Klauzolat kontraktuese standarde	☐
		Përkufizimi i mënyrës dhe kushteve për shkatërrimin e të dhënave	☐
		Mënyra e veprimit me të dhënat personale (revizionet, vizitat, etj.)	☐
14.	Sigurimi i shkëmbimit të të dhënave me organizatat e tjera	Enkriptimi i të dhënave përpara se t'i dërgoni	☐
		Sigurimi që informacioni do të arrijë vetëm tek ai që duhet ta lexojë	☐
		Dërgimi i çelësit sekret (fjalëkalimi ose ngjashëm) përmes kanalit tjetër	☐
15.	Siguria fizike	Zbatimi i qasjes restriktive në vendet e caktuara (salla e sistemit, arkivi, etj.)	☐
		Instalimi i alarmeve dhe kontrolli i rregullt i tyre	☐
16.	Mbikëqyrja e zhvillimit të softuerit	Ofrimi i parametrave që e respektojnë privatësinë e përdoruesve të fundit	☐
		Testimi i të dhënave anonime ose fiktive	☐
17.	Përdorimi i kriptografisë	Përdorimi i algoritmeve, softuerëve dhe bibliotekave të njohura	☐
		Ruajtja e informacioneve sekrete dhe çelësave kriptografikë në mënyrë të sigurt	☐

SHTOJCA 6 – ÇEKING-LISTA PËR FUSHAT KRYESORE TË VEPRIMIT NË LIDHJE ME IA DHE TË DREJTAT E NJERIUT

Vlerësimi i Ndikimit mbi të Drejtat e Njeriut	**Bëni këtë**
	Ndërmerrni hapa për të futur ligje dhe rregullativa që kërkojnë që VNDNJ-ja të zbatohet për sistemet e IA-së që ishin ose mund të jenë prokuruar, zhvilluar dhe/ose vënë në funksionim nga institucionet shtetërore. Kryeni në kohë VNDNJ për të gjitha sistemet e IA-së që tashmë janë vënë në funksionim / tashmë përdoren nga institucionet shtetërore në momentin kur miratohet korniza juridike relevante për VNDNJ. Përndryshe, VNDNJ duhet fillimisht të zbatohet përpara prokurimit dhe/ose zhvillimit të sistemit të IA-së nga institucioni shtetëror. Ndiqni vazhdimisht ndikimet e sistemit për IA-në mbi të drejtat e njeriut gjatë ciklit të tyre jetësor dhe kryeni VNDNJ të rregullta në çdo fazë të re të ciklit jetësor dhe kur ka ndryshime në kontekstin, fushëveprimin, natyrën dhe qëllimin e sistemeve.
	Mos e bëni këtë
	Mos harroni që të konsultoheni dhe të merrni informacione nga palët e interesuara relevante, duke përfshirë edhe organizatat e shoqërisë civile dhe ato me ekspertizë relevante për IA dhe të drejtat e njeriut, kur futni kornizë juridike për VNDNJ. Mos zbatoni VNDNJ në mënyrë jotransparente dhe mos përdorni ose lehtësoni përdorimin e ligjeve për konfidencialitet, privatësi, sekret pune, sekret shtetëror ose pronësi intelektuale për të parandaluar zbatimin ose publikimin e VNDNJ-së. Mos prokuroni, zhvilloni, vendosni në përdorim ose përdorni sistem për IA që ka potencialin të përzihet në të drejtat e njeriut në rrethanat kur (i) nuk ishte lëndë e VNDNJ-së ose (ii) VNDNJ zbulon se sistemi i IA-së paraqet rrezik real për shkeljen e të drejtave të njeriut dhe nuk janë zbatuar masat ose mekanizmat për të parandaluar ose zbutur rreziqet e identifikuara.
Konsultimi publik	**Bëni këtë**
	Zbatoni standarde për prokurime të hapura dhe proces transparent për përdorimin e sistemeve të IA-së. Përfshini të gjitha palët e interesuara në konsultimet publike, duke përfshirë edhe grupet ose komunitetet e interesuara, të paktën gjatë fazave të prokurimit dhe fazave të zbatimit të VNDNJ-së.

	Mos e bëni këtë
	Mos ofroni konsultime publike pa ndërmarrë masat përkatëse për t'i bërë të rëndësishme, duke përfshirë edhe publikimin paraprak në kohë të të gjitha informacioneve relevante në lidhje me sistemin e IA-së.

Informimi dhe transparenca	**Bëni këtë**
	Ofroni të gjitha informacionet e nevojshme në mënyrë që individët të kuptojnë se kur dhe si përdoren sistemet e IA-së, veçanërisht kur bëhet fjalë për shërbimet publike.
	Mos e bëni këtë
	Mos përdorni sisteme të IA-së që janë komplekse deri në shkallën që nuk mund të jenë lëndë e kontrollit të njeriut në përputhje me standardet përkatëse të transparencës dhe përgjegjësisë (llogaridhënies).
Mbrojtja e të dhënave personale dhe privatësisë	**Bëni këtë**
	Kryeni kontroll dhe vlerësim të ligjeve ekzistuese për mbrojtjen e të dhënave personale për të përcaktuar nëse ato mbrojnë mjaftueshëm të drejtën për respektimin e jetës private dhe të drejtën për mbrojtjen e të dhënave personale në kontekstin e sistemeve të IA-së. Ndërmerrni hapa në mënyrë proaktive për të siguruar që institucionet private dhe publike të përfshira në zhvillimin, vendosjen në përdorim dhe përdorimin e sistemeve të IA-së i respektojnë të drejtat e subjekteve të të dhënave personale dhe i përmbushin detyrimet e tyre në përputhje me ligjet në fuqi për mbrojtjen e të dhënave personale.
	Mos e bëni këtë
	Mos bëni përjashtime të mëdha dhe joproporcionale për ata që zhvillojnë, vendosin në përdorim ose përdorin sisteme të IA-së. Mos lejoni zhvillimin ose përdorimin e sistemeve të IA-së që mbështeten në trajnimin ose testimin e përmbledhjeve të të dhënave që ishin mbledhur ose përpunuar në mënyrë tjetër me shkeljen e së drejtës për respektimin e jetës private dhe së drejtës për mbrojtjen e të dhënave personale. Mos lejoni zhvillimin ose përdorimin e sistemeve të IA-së që përpunojnë të dhënat personale, qoftë si të dhëna hyrëse ose të dhëna dalëse, duke shkelur kështu të drejtën për respektimin e jetës private dhe të drejtën për mbrojtjen e të dhënave personale.

Për fund

Nëpërmjet përzgjedhjes së temave nga rregullativa për mbrojtjen e të dhënave personale në këtë Udhërrëfyes, jemi përpjekur të përpunojmë tituj që konsiderojmë se janë veçanërisht aktualë dhe të shpeshtë për zbatimin me sukses të detyrave dhe përgjegjësive që priten nga ju, si oficer për mbrojtjen e të dhënave personale.

Rekomandojmë që për udhëzime shtesë, si dhe përmbajtje të caktuara dhe të dobishme, që do të gjejnë zbatim të drejtpërdrejt praktik në punë, të përdorni faqen zyrtare të Agjencisë për Mbrojtjen e të Dhënave Personale, veçanërisht në pjesën e dedikuar për kontrollorin, si dhe dokumentin "Udhëzimet për oficerët për mbrojtjen e të dhënave personale" të miratuar nga Bordi Evropian për Mbrojtjen e të Dhënave Personale.

Punë të suksesshme dhe punoni në ndërtimin e cilësisë, kulturës dhe njohjes së pozicionit - oficer për mbrojtjen e të dhënave personale në institucionet tuaja.