METODOLOGJI PËR VLERËSIMIN E NDIKIMIT NDAJ PRIVATËSISË SË SHËRBIMEVE PUBLIKE QË JANË NË PROCES TË DIGJITALIZIMIT

METAMORPHOSIS
Fondacion për internet dhe shoqëri

KONEKT

METODOLOGJI PËR VLERËSIMIN E NDIKIMIT NDAJ PRIVATËSISË SË SHËRBIMEVE PUBLIKE QË JANË NË PROCES TË DIGJITALIZIMIT

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. QËLLIMI, FUSHËVEPRIMI DHE PËRDORUESIT

Me këtë Metodologji përshkruhet procedura e kryerjes së Vlerësimit të ndikimit ndaj privatësisë së shërbimeve publike të cilat janë në proces të digjitalizimit (më tutje: *VNMDHP*) në të gjitha institucionet publike (në tekstin e mëtutjeshëm: *"Institucionet"*), dhe Vlerësimi i ndikimit të cilin inteligjenca artificiale do ta ketë mbi privatësinë e qytetarëve, nëse zbatohet nga institucionet në procesin e ofrimit të shërbimeve publike.

Kjo metodologji e përshkruan metodën dhe i cakton hapat gjatë realizimit të VNMDHP-së dhe i siguron kriteret e nevojshme për vlerësim dhe shembuj referues.

Përdoruesit e këtij dokumenti janë Oficerët për mbrojtje të të dhënave personale dhe personat përgjegjës të njësive organizative në institucionit.

2. DOKUMENTE REFERUESE

- Ligji për mbrojtjen e të dhënave personale[1]
- Rregullorja për procesin e vlerësimit të ndikimit në mbrojtjen e të dhënave personale[2]
- Lista e llojeve të operacioneve të përpunimit për të cilat kërkohet realizimi i VNMDHP-së[3]
- Lista e llojeve të operacioneve të përpunimit për të cilat nuk kërkohet VNMDHP[4]
- Akti evropian për inteligjencë artificiale[5].

1 Ligji për mbrojtjen e të dhënave personale („Gazeta zyrtare e RMV-së" numër 42 nga 16.2.2020)

2 Rregullore për procesin e ndikimit në mbrojtjen e të dhënave personale („Gazeta zyrtare e Republikës së Maqedonisë së Veriut " nr. 122/20)

3 Lista e llojeve të operacioneve të përpunimit për të cilat kërkohet vleërsim të ndikimit mbi mbrojtjen e të dhënave personale („Gazeta zyrtare e Republikës së Maqedonisë së Veriut " nr. 122/20)

4 Lista e llojeve të operacioneve të përpunimit për të cilat nuk kërkohet vleërsim të ndikimit mbi mbrojtjen e të dhënave personale („Gazeta zyrtare e Republikës së Maqedonisë së Veriut " nr. 122/20)

5 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts

3. PËRKUFIZIME

Një pjesë e përkufizimeve të cekura të termeve të përdorura në këtë dokument janë në përputhje me Ligjin për mbrojtje të të dhënave personale, e një pjesë janë sqarim për ta kuptuar plotësisht këtë dokument:

Të dhënat personale: çdo informatë e cila ka të bëjë me personin e identifikuar fizik ose personin fizik i cili mund të identifikohet. Personi i identifikuar fizik është personi i cili mund të identifikohet në mënyrë të drejtpërdrejtë ose të tërthortë me përdorimin e informatave siç janë emri, numri i letërnjoftimit, lokacioni dhe informatat tjera, ose një ose më shumë faktorë të cilët janë specifikë për identitetin fizik, fiziologjik, psikologjik, ekonomik, kulturor ose social të personit. Në të dhënat personale bëjnë pjesë email adresat, numri telefonik, të dhënat biometrike (p.sh., gjurmët e gishtit), lokacioni, IP adresa, të dhënat shëndetësore, përkatësia fetare, statusi martesor dhe ngjashëm.

Kategoria e veçantë e të dhënave personale: Të dhënat personale që zbulojnë racë ose origjinë etnike, qëndrime politike, fetare ose bindje filozofike, anëtarësim në organizatat sindikale, të dhënat gjenetike, të dhënat biometrike, të dhënat shëndetësore, të dhënat për jetën seksuale ose përkatësinë seksuale.

Informacione (zyrtare) të punës: Të dhënat si emri dhe mbiemri, pozita e punës, numri telefonik zyrtar, adresa zyrtare, email adresa zyrtare, si dhe informatat tjera të ngjashme për personat që nuk janë për qëllim ekskluziv personal.

Kontrollori: Personi fizik ose juridik, organi i pushtetit shtetëror, organi shtetëror ose personi juridik i themeluar nga shteti për kryerje të autorizimeve publike, agjencia ose trup tjetër, i cili në mënyrë të mëvetësishme ose së bashku me tjerë i përcakton qëllimet dhe mënyrën e përpunimit të të dhënave personale, e kur qëllimet dhe mënyra e përpunimit të të dhënave personale janë përcaktuar me ligj, me ligjin e njëjtë përcaktohen kontrollori ose kriteret e veçanta për caktimin e tij.

Përpunuesi i përmbledhjes së të dhënave personale: Personi fizik ose juridik, organi i pushtetit shtetëror, organi shtetëror ose personi juridik i themeluar nga shteti për kryerje të autorizimeve publike, agjencia ose trup tjetër i cili i përpunon të dhënat personale në emër të kontrollorit. Shembuj për përpunues janë: kompania softuerike e cila mirëmban softuer për resurse njerëzore, provajderi i servisit "claud", kompania e angazhuar për mirëmbajtje të sistemit TI etj.

Vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale (VNMDHP): Procesi i parashikuar për t'i përshkruar aktivitetet e punës, për ta vlerësuar domosdoshmërinë dhe proporcionalitetin, dhe për të ndihmuar në përballjen me rreziqet që mund të paraqiten gjatë kryerjes së atyre aktiviteteve mbi të drejtat dhe liritë e personave fizikë. Shembuj për aktivitete për të cilat nevojitet të realizohet VNMDHP janë: përpunimi i vëllimshëm i kategorisë së veçantë të

të dhënave personale ose të dhënave personale lidhur me dënime ndëshkimore dhe veprat ndëshkimore, përpunimi i të dhënave personale me përdorimin e vëzhgimit (monitorimit) sistemor të hapësirës së disponueshme publike në përmasa të mëdha dhe ngjashëm.

Përpunimi i të dhënave personale: çdo operacion ose përmbledhje të operacioneve që kryhen mbi të dhënat personale, ose mbi grupin e të dhënave personale, në mënyrë automatike ose në mënyrë tjetër. Me operacion/e nënkuptohet: mbledhje, evidentim, organizim, strukturim, ruajtje, përshtatje ose ndryshim, tërheqje, konsultim, kontroll, përdorim, zbulim përmes transferimit, publikimit ose në mënyrë tjetër disponueshmërisë, harmonizimit ose kombinimit, kufizimit, fshirjes ose shkatërrimit.

Digjitalizimi: procesi i shndërrimit të informatave në format digjital (përkatësisht në format të lexueshëm kompjuterik)

Inteligjenca artificiale (IA): inteligjenca e demonstruar nga makinat, veçanërisht nga sistemi kompjuterik. Detyrat të cilat do t'i kryejë IA janë zgjidhja e problemeve, perceptimi vizual, njohja e zërit, miratimi i vendimeve, përkthimet dhe ngjashëm.

4. UDHËZIME KRYESORE

Metodologjia për VNMDHP është dokument i cili u mundëson institucioneve si kontrollorë, dhe bartës të aktiviteteve (operacioneve)[6] për përpunimin e të dhënave personale t'i identifikojnë rreziqet lidhur me përpunimin e të dhënave personale dhe obligimet e tyre për futje të masave për mbrojtje të të drejtave dhe lirive të subjekteve të të dhënave personale.

Obligimi për realizimin e VNMDHP-së i referohet çdo kontrollori. Kur përpunimi do të realizohet plotësisht ose pjesërisht nga përpunuesi, atëherë përpunuesi duhet t'i ndihmojë kontrollorit në realizimin e VNMDHP-së me ç'rast rolet, obligimet dhe përgjegjësitë e kontrollorit dhe përpunuesit do të përcaktohen në marrëveshje të ndërsjellë, në përputhje me rregullat për mbrojtjen e të dhënave personale.

Procesi i VNMDHP-së në vete bart përfitime të mëdha si për kontrollorin, ashtu edhe për përpunuesin. Gjegjësisht, ky proces merr parasysh privatësinë dhe mbrojtjen e të dhënave personale dhe parasheh implementim të masave teknike

6 *Në kuadër të dokumentit të plotë do të përdoren terminët aktivitete dhe operacione për përpunim të të dhënave personale që dalin nga Ligji për mbrojtje të të dhënave personale dhe Rregullorja për procesin e vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale.*

dhe organizative adekuate, përkatësisht aktivitete qëllimi i të cilave është sigurimi i fshehtësisë dhe mbrojtjes së të dhënave, që në momentin e përcaktimit të mjeteve për përpunim. Përfitimet nga realizimi i VNMDHP-së përfshijnë: instalim të sistemit për paralajmërim të hershëm, miratim të vendimeve të informuara, parandalim dhe minimizim të rreziqeve për cenim të privatësisë dhe mbrojtje të të dhënave personale.

VNMDHP-ja realizohet para se të fillojë përpunimi i të dhënave personale dhe kur sipas natyrës, vëllimit, kontekstit dhe qëllimeve të përpunimit ekziston gjasë për t'u shkaktuar rrezik i lartë mbi të drejtat dhe liritë e personave fizikë, e veçanërisht kur futen teknologji të reja për përpunim të të dhënave personale.

VNMDHP-ja detyrimisht realizohet në rast të:

- përpunimit të vëllimshëm të kategorive të veçanta të të dhënave personale;
- vëzhgimit sistemor të hapësirave të disponueshme publike në përmasa të mëdha;
- vlerësimit sistemor dhe gjithëpërfshirës të aspekteve personale që janë të lidhura me persona fizikë, i cili bazohet në përpunimin automatik përfshirë edhe profilizimin, e në bazë të të cilit miratohen vendime dhe kanë veprim juridik dhe ndikim të dukshëm ndaj personit fizik.
- Realizimi i VNMDHP-së është i detyrueshëm edhe në rast të transferimit të të dhënave në "claud", futjes së produktit të ri, përpunimit të të dhënave për qëllimin i cili është i ndryshëm nga qëllimi i përcaktuar fillestar, fillimit të bashkëpunimit me furnizues të rinj të shërbimeve, futjes së profilizimit të klientëve, transferimit të të dhënave personale në vendet e treta, aspekteve të reja të sigurisë së informacionit dhe ngjashëm. Përveç në rastet e cekura, VNMDHP-ja realizohet në përputhje me "Listën e llojeve të operacioneve për përpunim për të cilat kërkohet Vlerësim të ndikimit mbi mbrojtjen e të dhënave personale"[7] të miratuar nga Agjencia për Mbrojtjen e të Dhënave Personale (në tekstin e mëtutjeshëm: AMDHP).
- VNMDHP-ja nuk kërkohet për lloje të caktuara të operacioneve të përpunimit, veçanërisht:
- Për operacionet për përpunim të rezultateve me rrezik të lartë për të drejtat dhe liritë e personave fizikë;
- Kur aktivitetet (operacionet) kanë qenë të përcaktuara paraprakisht se nuk janë të ekspozuara ndaj rrezikut gjatë vlerësimit të kryer të ndikimit mbi mbrojtjen e të dhënave personale;

7 Lista e llojeve të operacioneve për përpunim për të cilat kërkohet Vlerësim të ndikimit mbi mbi mbrojtjen e të dhënave personale (Gazeta zyrtare e RMV-së, nr.122 nga 12.05.2020).

- Kur përpunimi tashmë është miratuar nga AMDHP-ja.
- Përveç në rastet e cekura, VNMDHP-ja nuk realizohet në përputhje me "Listën e llojeve të operacioneve për përpunim për të cilat nuk kërkohet vlerësim të ndikimit mbi mbrojtjen e të dhënave personale" [8]të miratuar nga AMDHP-ja. Gjatë kryerjes së vlerësimit të ndikimit mbi mbrojtjen e të dhënave personale, përdoret Raporti për VNMDHP (Shtojca nr. 1 e kësaj Metodologjie). Raporti për VNMDHP përdoret për mbledhje të të dhënave, vlerësim të rreziqeve, përcaktim të masave për reduktim të rrezikut dhe për njoftim për rezultatet nga VNMDHP-ja e realizuar.
- Në raste kur ka kontrollorë të përbashkët, secili kontroll doemos duhet të përcaktojë se ku përket cila pjesë e aktiviteteve të përpunimit të të dhënave personale.

5. PERSONAT PËRGJEGJËS

Në VNMDHP janë përfshirë personat në vijim:

- **Oficeri për mbrojtje të të dhënave personale**

Oficeri për mbrojtje të të dhënave personale lidhur me aktivitetet për përpunim dhe VNMDHP jep rekomandime, mendime dhe këshilla të cilat i rregullojnë çështjet në vijim:

1. A është i detyrueshëm realizimi i VNMDHP-së?
2. Si të realizohet VNMDHP-ja?
3. Zgjedhja e metodologjisë për VNMDHP-në.

Oficeri për mbrojtjen e të dhënave personale është personi i cili detyrimisht jep mendim edhe lidhur me dokumentacionin e përgatitur gjatë realizimit të VNMDHP-së.

- **Personi përgjegjës i aktivitetit për përpunimin e të dhënave personale (pronar i procesit) është personi përgjegjës në kompetenca të të cilave bën pjesë aktiviteti i cili duhet të realizohet ose personi tjetër i autorizuar (p.sh., udhëheqësi i sektorit/shërbimit/seksionit).**

VNMDHP-në e realizojnë personat përgjegjës nga njësitë afariste ku bën pjesë aktiviteti për përpunim të të dhënave personale për të cilat nevojitet të

8 Lista e llojeve të operacioneve për përpunim për të cilat nuk kërkohet Vlerësim të ndikimit mbi mbrojtjen e të dhënave personale (Gazeta zyrtare e RMV-së, nr.122 nga 12.05.2020).

realizohet VNMDHP-ja. Sipas udhëzimeve të kësaj Metodologjie, i njëjti bëhet në bashkëpunim me Oficerin për mbrojtje të të dhënave personale. Gjatë realizimit përfshihen edhe njësitë tjera organizative në institucionin të cilat janë të lidhura me aktivitetin për përpunim me të cilin planifikohet të bëhet përpunimi i të dhënave personale.

- **Konsulenti** – sipas nevojës, institucioni do të angazhojë persona të jashtëm ose ekspertë të pavarur, në përputhje me natyrën e zgjidhjeve teknologjike dhe organizative të cilat do të aplikohen gjatë aktivitetit të përpunimit të të dhënave personale.

6. FAZAT PËR REALIZIMIN E VNMDHP-SË

6.1 Faza 1: Pyetësori kualifikues

Oficeri për mbrojtjen e të dhënave personale së bashku me personin përgjegjës për aktivitetin për përpunim të të dhënave personale do t'u përgjigjen pyetjeve kualifikuese nga Raporti për VNMDHP. Këto pyetje janë të domosdoshme që të përcaktohet nëse aktiviteti konkret për përpunimin e të dhënave personale është me rrezik të lartë mbi të drejtat dhe liritë e personave fizikë.

Oficeri për mbrojtjen e të dhënave personale, në bazë të pyetësorit kualifikues, do të konstatojë nëse aktiviteti konkret për përpunimin e të dhënave personale duhet të vazhdojë me fazat vijuese, përkatësisht të realizohet VNMDHP. Nëse të paktën për një prej pyetjeve kualifikuese nga faza 1 të Raportit për VNMDHP është përgjigjur me "PO", atëherë për atë aktivitet për përpunimin e të dhënave personale duhet të vazhdohet me fazat në vijim. Krahas aktiviteteve të përcaktuara në bazë të pyetësorit kualifikues, për aktivitete të caktuara duhet të realizohet VNMDHP sepse gjenden në Listën e llojeve të operacioneve për përpunim për të cilat kërkohet VNMDHP (Shtojca nr. 2 nga kjo Metodologji).

Pyetësori i përgjigjur kualifikues së bashku me dokumentacionin (oferta, propozim-kontrata, shërbimi dhe ngjashëm) i dorëzohet Oficerit për mbrojtje të të dhënave personale.

Nëse në bazë të pyetjeve kualifikuese konstatohet se nuk ka nevojë për realizimin e VNMDHP-së, aktiviteti nuk gjendet në Listën e llojeve të operacioneve për përpunim për të cilat kërkohet VNMDHP, megjithatë, Oficeri për mbrojtje të të dhënave personale mund të vendosë të realizohet VNMDHP-ja, nëse konsideron se institucioni duhet të marrë një pasqyrë më të qartë të rreziqeve që mund të ndodhin.

Përjashtim janë aktivitetet të cilat janë përfshirë me Listën e llojeve të operacioneve për përpunim për të cilat nuk kërkohet VNMDHP (Shtojca nr. 3 nga kjo Metodologji). Oficeri për mbrojtje të të dhënave personale është i detyruar që të monitorojë nëse në listat nga Shtojcat 2 dhe 3 të kësaj Metodologjie, disa aktivitete janë shtuar/mënjanuar.

6.2 Faza 2: Përshkrimi i aktivitetit për përpunimin e të dhënave personale

Personi përgjegjës i aktivitetit për përpunimin e të dhënave personale duhet t'i japë përshkrim të plotë aktivitetit për përpunimin e të dhënave personale. Konkretisht, duhet t'i japë përshkrim natyrës, fushëveprimit, kontekstit dhe qëllimit të aktivitetit, e me qëllim të fitimit të një pasqyre më të qartë dhe më precize të aktivitetit të planifikuar. E gjithë kjo do të kontribuojë për kompletimin e fazave vijuese.

Në këtë fazë përcaktohet konteksti i përpunimit dhe ceken, përkatësisht përshkruhen së paku informatat në vijim:

- Aktiviteti për përpunimin e të dhënave personale;
- Qëllimi i përpunimit;
- Lëvizja e të dhënave;
- Metoda(t) e marrjes së të dhënave;
- Mënyra dhe mjetet për përpunimin e të dhënave (pajisja e përdorur, rrjetet, resurset njerëzore etj);
- Subjektet që janë përfshirë në përpunimin (kontrollorë, përpunues, përdorues etj);
- Afati i ruajtjes.

6.3 Faza 3: Konsultimi

Në këtë fazë, nevojitet të përcaktohet se kush do të konsultohet për kryerjen e aktivitetit për përpunimin e të dhënave personale. Oficeri për mbrojtje të të dhënave personale vendos nëse dhe kur do të kërkojë mendim nga subjektet e të dhënave personale të dhënat e të cilave do të përfshihen me aktivitetin.

Mendimi nga subjektet e të dhënave personale ose përfaqësuesit e tyre, mund të kërkohen përmes metodave të ndryshme, varësisht nga konteksti (për shembull, studimi i përgjithshëm lidhur me qëllimin dhe mjetet e aktivitetit për përpunim, duke u parashtruar pyetje përfaqësuesve të subjekteve të të dhënave personale,

ose përmes anketave që u dërgohen klientëve të ardhshëm të kontrollorit).

Nëse vendimi final i institucionit dallohet nga mendimi i subjekteve të të dhënave personale, shkaqet për vazhdimin ose ndërprerjen e përpunimit të të dhënave personale detyrimisht duhet të arsyetohen në Raportin për VNMDHP. Nëse institucioni vendos të mos kërkojë mendim nga subjektet e të dhënave personale (për shembull: nëse me atë do të rrezikohet konfidencialiteti i planeve të punës në institucionin ose ai nuk është proporcional dhe/ose nuk është i realizueshëm), arsyetimi për vendimin e tillë duhet të dokumentohet në Raportin për VNMDHP.

Gjithashtu, është e mundshme përfshirja edhe e palëve tjera të cilat do të konsultohen për aktivitetin, siç janë konsulentët me ekspertizë të ndryshme ose përpunuesit.

6.4 Faza 4: Vlerësimi i domosdoshmërisë dhe proporcionalitetit

Për aktivitetin e përpunimit të dhënave personale për të cilin nevojitet VNMDHP, personi përgjegjës i aktivitetit për përpunimin e të dhënave personale e plotëson Raportin për VNMDHP. Sipas nevojës, personi përgjegjës mund të kërkojë ndihmë dhe mbështetje për këtë fazë nga Oficeri për mbrojtjen e të dhënave personale. Qëllimi i kësaj faze është të argumentohet nevoja për aktivitetin e tillë, përkatësisht të argumentohet domosdoshmëria e saj dhe të përcaktohet nëse është paraparë përdorimi i të dhënave personale në një shkallë proporcionalisht me qëllimin.

Oficeri për mbrojtjen e të dhënave personale e kontrollon pyetësorin kualifikues së bashku me dokumentacionin shoqërues dhe mund të kërkojë sqarim plotësues ose të parashtrojë pyetje plotësuese që të qartësohen të gjitha aspektet nga përpunimi i planifikuar i të dhënave personale.

Personi përgjegjës i aktivitetit për përpunim i cili ka për obligim të realizojë VNMDHP, është i detyruar që nga ofertuesit potencialë t'i sigurojë të gjitha të dhënat për shërbimin të cilin e ofrojnë dhe ta marrë dokumentacionin relevant lidhur me përpunimin e të dhënave personale të të gjithë nënpërpunuesve (kushte të përgjithshme, kontrata, masa sigurie, VNMDHP-ja ekzistuese e nënpërpunuesve etj).

6.5 Faza 5: Identifikimi dhe vlerësimi i rreziqeve

Në këtë fazë, personi përgjegjës i aktivitetit për përpunimin e të dhënave personale duhet t'i identifikojë kërcënimet të cilat mund të ndodhin dhe ta rrezikojnë sigurinë e të dhënave personale, përkatësisht t'i rrezikojë të drejtat

dhe liritë e personave fizikë. Gjithashtu në këtë fazë duhet të identifikohet probabiliteti dhe ndikimi nëse realizohen këto kërcënime.

Gjatë përcaktimit të rreziqeve të cilat janë të lidhura me përpunimin, veçanërisht do të merren parasysh rreziqet që mund të kontribuojnë për shkatërrim të rastësishëm ose joligjor, humbje, ndryshim, zbulim të paautorizuar të të dhënave personale ose qasje të paautorizuar ndaj të dhënave personale të transferuara, të ruajtura ose në mënyrë tjetër të përpunuara.

Ndikimi (pasoja në rast të realizimit të kërcënimit) mund të jetë:

- **i ulët,** kur personat fizikë mund të përballen me disa pakëndshmëri, të cilat do t'i tejkalojnë pa problem;
- **i mesëm,** kur personat fizikë mund të përballen me pakëndshmëri të dukshme, të cilat do të mund t'i tejkalojnë edhe krahas vështirësive të caktuara;
- **i lartë,** kur personat fizikë mund të përballen me pasoja të dukshme, të cilat duhet të jenë në gjendje t'i tejkalojnë, por me vështirësi serioze; dhe
- **shumë i lartë,** kur personat fizikë mund të përballen me pasoja të konsiderueshme, bile edhe me pasoja të pakthyeshme, të cilat me gjasë nuk do të mund t'i tejkalojnë.
- Probabiliteti (kërcënim i caktuar për të ndodhur për shkak të mungesës ose dobësisë së kontrolleve), mund të jetë:
- **i ulët** – është e pritshme që kërcënimi/ngjarja të realizohet njëherë në vit ose më rrallë;
- **i mesëm –** e pritshme që kërcënimi/ngjarja të realizohet në gjashtë muaj ose më rrallë;
- **i lartë** – është e pritshme që kërcënimi/ngjarja të realizohet njëherë në muaj.

Vlera e probabilitetit dhe ndikimit përcaktohet në bazë të analizës së parametrave në vijim:

- Vlera e aktivitetit për përpunim të cilit i referohet rreziku, përkatësisht kërcënimi;
- Vulnerabilitetet e aktivitetit për përpunim të cilat mundësojnë realizim të rrezikut, përkatësisht kërcënimeve;
- Përvojat paraprake dhe trendët globalë dhe rajonalë lidhur me kërcënimin e identifikuar;
- Kontrollet ekzistuese të sigurisë të realizuara ndaj resurseve të informacionit të cilat janë pjesë e aktivitetit për përpunim.

Rreziku i përgjithshëm përllogaritet si funksion i probabilitetit për të ndodhur kërcënimi dhe ndikimi (pasoja) të cilin mund ta ketë ai kërcënim.

Rreziku – probabiliteti x ndikimi

Probabiliteti	**Matrica e rrezikut**			
L (Lartë)	**U**	**M**	**L**	**SHL**
M (Mesëm)	**U**	**M**	**L**	**SHL**
U (Ulët)	**U**	**U**	**M**	**L**
Ndikimi	**U** (ulët)	**M** (Mesëm)	**L** (Lartë)	**SHL** (Shumë i lartë)

6.6 Faza 6: Përcaktimi i masave për reduktim të rreziqeve

Pasi të identifikohen rreziqet, Oficeri për mbrojtjen e të dhënave personale në bashkëpunim me personin përgjegjës për aktivitetin e përpunimit të të dhënave personale, e sipas nevojës edhe në bashkëpunim me personat përgjegjës për sistemin e informacionit dhe sigurinë e tij, do të përcaktojnë masa mbrojtëse për reduktim të rreziqeve. Detyrimisht trajtohen rreziqet të cilat nga përllogaritja janë treguar me rrezik të përgjithshëm i mesëm, i lartë ose shumë i lartë.

Plani për përballje me rreziqet do të përfshihet në Raportin për VNMDHP. Detyrimisht duhet të ceken informatat në vijim:

- Masat e sigurisë të cilat duhet të zbatohen për menaxhimin e rrezikut:

Në vazhdim, shembulli i masave të cilat mund të zbatohen në përputhje me parimet për mbrojtjen e të dhënave personale.

Në përputhje me parimin e ligjshmërisë, drejtësisë dhe transparencës – Përkufizimi i Politikës së privatësisë, trajnimi dhe rritja e vetëdijes së punonjësve lidhur me mbrojtjen e të dhënave personale, forma adekuate e pëlqimit dhe mundësia për tërheqjen e tij, baza juridike adekuate për përpunim, informimi i subjektit (subjekti është njoftuar në kohë se cilat të dhëna personale do të përpunohen, për cilat qëllime, kush do t'i përpunojë, kujt mund t'i drejtohet, afati i ruajtjes, të drejtat e subjektit), veprimi në kohë me kërkesë të subjektit etj.

Në përputhje me parimin e kufizimit të qëllimeve – Mbledhja dhe përpunimi i të dhënave personale vetëm për qëllime të përcaktuara saktësisht. Për shembull të informohen dhe trajnohen personat të cilët përpunojnë të dhëna personale dhe që kanë qasje në to se të dhënat personale të mbledhura për një qëllim nuk guxojnë të përdoren për qëllime tjera, për shembull profilizimi, zbulimi i paautorizuar etj.

Në përputhje me parimin e vëllimit minimal të të dhënave – Përcaktimi i sasisë minimale të të dhënave e cila është e nevojshme për përmbushjen e qëllimit (nuk është adekuate të mblidhen të dhëna plotësuese të cilat nuk nevojiten për arritjen e qëllimit), pseudonimizimi etj.

Në përputhje me parimin e saktësisë – Nevojitet të përcaktohen masa me të cilat të dhënat e mbledhura janë të sakta dhe të përditësuara në çdo moment, që t'i jepet mundësi subjektit për ta realizuar të drejtën e tij për korrigjim të të dhënave të cilat janë të pasakta dhe jo të plota.

Në përputhje me parimin e kufizimit të afatit të ruajtjes – Nevojitet procedurë adekuate për fshirje ose shkatërrim të të dhënave personale pas skadimit të afatit për ruajtjen e tyre. Futja e masave teknike për fshirje të automatizuar pas afatit të përcaktuar të ruajtjes së të dhënave personale.

Në përputhje me parimin e integritetit dhe konfidencialitetit – Aplikimi i procedurave të miratuara të TI-së për masa teknike dhe organizative (kriptimi i pajisjes, kriptimi i bazave të të dhënave, pseudonimizimi, kontrolli fizik i qasjes, qasja në të dhënat e kufizuar vetëm në të punësuarit, përdorimi i fjalëkalimeve "të fuqishme", kontrollimi i autenticitetit, kopjet e sigurisë, firewall, etj), siguri TI, njoftim në kohë për cenimin e sigurisë (humbja, publikimi, qasja e paautorizuar), parandalimi i incidenteve, etj.).

Në përputhje me parimin e llogaridhënies – Respektimi i dispozitave për përpunim të të dhënave personale, rregullat dhe procedurat e përcaktuara për përpunimin e të dhënave personale, transferimin adekuat të të dhënave personale, trajnimin e të punësuarve në institucionin për punë të kujdesshme, preventive dhe proaktive.

Masat e sigurisë duhet të zbatohen edhe ndaj të dhënave personale të cilat do të transferohen në vendet e treta (jashtë BE-së, shembull: ruajtja në server). Duhet të përcaktohet se cili është shkaku dhe cilat të dhëna personale do të transferohen jashtë BE-së, si dhe cilat masa do të ndërmerren gjatë transferimit të të dhënave personale. A do të rregullohet transferimi i të dhënave personale me marrëveshje ndërkombëtare, vendim për përshtatshmëri nga AMDHP-ja ose komisioni evropian ose me pëlqim të qartë të subjektit të të dhënave personale?

Masa për mbrojtjen e të dhënave personale gjatë transferimit në vendet e treta:

- klauzola standarde e Marrëveshjes për mbrojtje të të dhënave personale të cilat i përcakton AMDHP-ja[9] ose janë miratuar nga Komisioni Evropian (ang. SCC – standard contractual clauses[10]);
- rregulla të detyrueshme korporative;

9 Klauzola kontraktuese standarde (AMDHP)
10 Standard contractual clauses for international transfers (European Commission)

- detyrime të miratuara obligative dhe ekzekutive të kontrollorit ose përpunuesit në vendin e tretë për aplikim të masave adekuate të sigurisë dhe mbrojtje të të drejtave të subjekteve të të dhënave personale;
- Personat përgjegjës për implementimin e masave (Oficeri për mbrojtjen e të dhënave personale, personi përgjegjës i aktivitetit për përpunim të të dhënave personale [pronar i procesit – udhëheqës i sektorit] dhe konsulent [personi i angazhuar i jashtëm ose ekspertët e pavarur]);
- Afatet për zbatim të masave për reduktim të rreziqeve të identifikuara.

6.7 Faza 7: Shënim për zbatimin e masave të sigurisë

Masat e sigurisë të cilat që janë zbatuar duhet të evidentohen në Raportin për VNMDHP në kolonën "Shënim për përfundim".

7. KONSULTIMI PARAPRAK ME AGJENCINË PËR MBROJTJE TË TË DHËNAVE PERSONALE

Nëse rezultatet nga VNMDHP-ja tregojnë se aktiviteti për përpunimin e të dhënave personale është me rrezik të lartë pasi të zbatohen masat e sigurisë, ndërsa institucioni ka interes për ta kryer aktivitetin në fjalë për përpunimin e të dhënave personale, atëherë Oficeri për mbrojtjen e të dhënave personale doemos duhet të konsultohet me AMDHP-në para se të fillojë kryerja e aktivitetit në fjalë.

Pa marrë parasysh rezultatin nga VNMDHP-ja, përkatësisht për çdo rrezik (i ulët, i mesëm, i lartë ose shumë i lartë), institucioni do të kërkojë miratim paraprak nga AMDHP-ja që të mund të kryejë përpunim të të dhënave personale për qëllimet e interesit publik, përfshirë edhe përpunimin për qëllimet e mbrojtjes sociale dhe shëndetësisë publike. Miratimi i tillë, veçanërisht do të kërkohet në rast kur:

- aktivitetet themelore të institucionit përbëhen nga operacionet për përpunim, të cilat për shkak të natyrës, fushëveprimit dhe/ose qëllimeve të tyre kërkojnë në masë të madhe monitorim të rregullt dhe sistemor të subjekteve të të dhënave personale;
- aktivitetet themelore të institucionit përbëhen nga përpunimi i vëllimshëm i kategorive të veçanta të të dhënave personale ose të dhënave personale lidhur me dënimet ndëshkimore dhe veprat ndëshkimore;

do të bëhet vëzhgimi sistemor i hapësirave ose hapësirave në përmasa të mëdha.

AMDHP-ja do të konsultohet nga institucioni gjatë përpunimit të propozim-ligjeve ose akteve nënligjore të cilat miratohen në bazë të atyre ligjeve, e që kanë të bëjnë me përpunimin e të dhënave personale.

Oficeri për mbrojtjen e të dhënave personale do t'ia sigurojë AMDHP-së informatat në vijim:

- Përgjegjësitë e kontrollorit, kontrollorit(ëve) dhe përpunuesit(ve);
- Qëllimet dhe mjetet e përpunimit të planifikuar;
- Masat e parapara të sigurisë për përpunimin e të dhënave personale;
- Të dhënat kontaktuese të Oficerit për mbrojtjen e të dhënave personale; dhe
- Raporti nga VNMDHP-ja.

8. RISHIKIMI I RREGULLT I VNMDHP-SË

Oficeri për mbrojtjen e të dhënave personale doemos duhet ta rishikojë VNMDHP-në në njërin prej rasteve në vijim:

- Nëse ndryshohen rreziqet lidhur me aktivitetet për përpunimin e të dhënave personale, (p.sh. ndonjë prej rreziqeve ka kaluar nga niveli i mesëm në nivelin e lartë);
- Nëse ka ndryshim të konsiderueshëm në aktivitetet për përpunimin e të dhënave personale (p.sh. nëse ndryshohen lënda, qëllimi dhe mënyrat e përpunimit të të dhënave personale);
- Nëse ndodh ndryshim në masat teknike dhe organizative (p.sh., nëse implementohet ndonjë softuer, sistem i ri etj);
- Nëse paraqitet nevojë për transferim ndërkufitar të të dhënave (p.sh. ndonjë prej aktiviteteve parasheh transferim të të dhënave personale gjatë përdorimit të shërbimeve në "claud" në shtetet e BE-së, Hapësirën ekonomike evropiane (HEE) ose në vendet e treta);
- Nëse ka ndryshim në kërkesat ligjore (ndryshim të ligjit në bazë të të cilit realizohet përpunimi i të dhënave personale); ose
- Nëse institucioni vepron si përpunues, ndërsa kontrollori kërkon që NVMDHP të rishikohet etj.

9. VLERËSIMI I NDIKIMIT TË CILIN INTELIGJENCA ARTIFICIALE DO TA KETË MBI PRIVATËSINË E QYTETARËVE[11]

Çdo ditë, inteligjenca artificiale (në tekstin e mëtejmë: IA) ndryshon mënyrën se si ne e përjetojmë botën. Tashmë përdorim IA për të gjetur rrugën më të shkurtër dhe më të shpejtë për në shtëpi, për të na paralajmëruar për aktivitete të dyshimta në llogaritë tona bankare dhe për të filtruar emailet spam.

Për qytetarët, aplikimi i teknologjive për IA do të rezultojë me një përvojë më të personalizuar dhe më efikase. Për njerëzit që punojnë në sektorin publik kjo do të thotë reduktim i orëve që i kalojnë në detyrat kryesore, duke u dhënë atyre më shumë kohë për të shpenzuar në mënyra inovative për përmirësimin e shërbimeve

Përdorimet potenciale të IA në sektorin publik janë të rëndësishme, por doemos duhet të jenë të balancuara me mendime etike, të drejta dhe të sigurta.

IA është fushë hulumtuese e cila e përfshin filozofinë, logjikën, statistikën, shkencat kompjuterike, matematikën, nauroshkencën, linguistikën, psikologjinë kognitive dhe ekonominë.

Diskutimi ndërmjet përparësive të teknologjisë IA dhe rreziqeve për të drejtat tona të njeriut bëhet më i dukshëm në fushën e privatësisë. Privatësia është e drejtë themelore e njeriut, thelbësore për të jetuar me dinjitet dhe siguri. Por në mjedisin digjital, përfshirë kur përdorim aplikacione dhe platforma të mediave sociale, grumbullohen sasi të mëdha të të dhënave personale - me ose pa dijeninë tonë - dhe mund të përdoren për të na profilizuar dhe për të bërë parashikime për sjelljen tonë. Ne publikojmë të dhëna për shëndetin tonë, idetë politike dhe jetën familjare pa e ditur se kush do t'i përdorë këto të dhëna, për çfarë qëllimesh dhe pse.

Makineritë funksionojnë në bazë të asaj që ua thonë njerëzve. Nëse sistemi ushqehet me paragjykime njerëzore (të vetëdijshme ose të pavetëdijshme), rezultati në mënyrë të pashmangshme do të jetë i njëanshëm. Ekziston mangësi në diversitetin dhe në përfshirjen në hartimin e sistemeve për IA: në vend që vendimet tona të jenë më objektive, ato mund t'i përforcojnë diskriminimin dhe paragjykimet.

11 *Ky proces ende nuk është rregulluar në Republikën e Maqedonisë së Veriut. Janë shfrytëzuar materiale nga Akti evropian për inteligjencë artificiale i miratuar nga Parlamenti Evropian më datë 14.06.2023 dhe materiale tjera që e rregullojnë këtë materie.*

9.1 Përkufizime:

- Sipas Aktit për inteligjencë[12] (në tekstin e mëtutjeshëm: Akti) përkufizimi për ***"sistemin për inteligjencë artificiale" (sistemi për IA)*** *do të thotë "softuer i cili është zhvilluar me një ose më shumë prej teknikave dhe qasjeve të cekura në Aneksin I të Aktit (Shtojca nr. 4 e kësaj Metodologjie) dhe mund që për një set të dhënë të qëllimeve të përcaktuara nga njeriu, të gjenerojë rezultate siç janë përmbajtja, parashikimet, rekomandimet, ose vendimet të cilat ndikojnë në mjedise me të cilat ato komunikojnë";* megjithëse në përputhje me Aktin nga Parlamenti Evropian nga qershori 2023 përkufizimet janë pikë kontestuese e diskutimit që theksojnë se përkufizimi i sistemeve për IA është goxha i gjerë dhe do të përfshijë shumë më tepër sesa ajo që nënkuptohet në mënyrë subjektive si IA, përfshirë edhe algoritmet më të thjeshta për kërkim, klasifikim dhe rutim, të cilat në mënyrë sukcesive do të jenë objekt i rregullave të reja;
- ***"provajder ose ofrues"*** *do të thotë personi juridik ose fizik, institucioni shtetëror, agjencia ose trupi tjetër i cili zhvillon sistem për IA ose që ka zhvilluar sistem për IA me qëllim për ta plasuar në tregun ose ta vë në përdorim nën emrin e tij ose shenjën mbrojtëse, pa marrë parasysh nëse ai do të jetë me pagesë ose falas;*
- *"**përdorues"** do të thotë çdo person fizik ose juridik, institucion shtetëror, agjenci ose trup tjetër i cili përdor sistem për IA nën kompetencën e tij, përveç kur sistemi për IA përdoret gjatë aktivitetit joprofesional personal.*

Duhet bërë dallim lidhur me detyrimet ndërmjet provajderit dhe përdoruesit të sistemit të dhënë me rrezik të lartë për IA. Provajderët janë qëllim primar lidhur me harmonizimin, si dhe detyrimet në përputhje me Aktin për IA. Përveç që duhet t'i përmbushin kërkesat e poshtëshënuara, kanë edhe detyrime për bashkëpunim dhe sigurim të informatave ndaj përdoruesve nën rrethana të caktuara. Krahas provajderëve, importuesve dhe shpërndarësve të sistemeve IA kanë detyrime të caktuara sipas nenit 26 dhe 27 të Aktit. Këto detyrime, megjithatë, shpesh janë për konfirmim, verifikim dhe për qëllimet e sigurimit të informatave.

Detyrimet e përdoruesve janë paraparë në nenin 29 të Aktit sipas të cilit përdoruesit do të përdorin sisteme me rrezik të lartë për IA në përputhje me udhëzimet, do të realizojnë mbikëqyrje njerëzore dhe monitorim të punës së sistemit me rrezik të lartë për IA, do t'i marrë parasysh dispozitat për mbrojtje të të dhënave dhe do të bashkëpunojë me organet kombëtare.

12 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts

9.2 Akti evropian i inteligjencës artificiale

Duke e pasur parasysh këtë, Komisioni Evropian në prill 2021 e parashtroi propozim-Aktin Evropian për IA, të cilin deputetët e Parlamentit Evropian e miratuan dy vite më vonë, në qershor 2023.

Draft-akti për IA është përpjekja e parë për të miratuar një rregullore horizontale për IA. Korniza ligjore e rregullon përdorimin e sistemeve për IA dhe rreziqet e lidhura. Komisioni propozon vendosjen e një përkufizimi teknologjik neutral të sistemeve për IA dhe të përcaktohet klasifikim i sistemeve për IA, ku secili grup do të ketë kushte dhe detyrime të ndryshme të cilat do të përcaktohen në bazë të një „qasjeje të bazuar në rrezik". Sistemet për IA që rezultojnë në një nivel „të papranueshëm" rreziku do të ndalohen. Një numër i madh i sistemeve për IA me rrezik të lartë do të lejohen për përdorim, por ato do të duhet të përmbushin disa kushte dhe detyrime për të fituar qasje në tregun e BE-së. Ato sisteme për IA që rezultojnë me një nivel „të kufizuar" rreziku do të jenë objekt i detyrimeve të thjeshta të transparencës.

Pozicioni kryesor i shteteve anëtare të BE-së në dhjetor 2021 u prezantua nga Këshilli i BE-së dhe Parlamenti votoi për pozicionin e tij e tij në qershor 2023. Deputetët e BE-së i filluan negociatat për finalizimin e legjislacionit të ri, me ndryshime të konsiderueshme të propozimit të Komisionit, duke përfshirë rishikimin e përkufizimit të sistemev IA, zgjerimin e listës së sistemeve të AI të ndaluara dhe imponimin e detyrimeve për IA për dedikim të përgjithshëm dhe modele gjeneruese të IA siç është ChatGPT[13]

9.3 Inteligjenca artificiale dhe ndikimi i saj mbi të drejtat e qytetarëve

IA në vitet e fundit shënon progres të shpejtë, ndërsa me zhvillimin e saj mundëson aplikim më të madh në të gjitha sferat e shoqërisë që kontribuon për përmirësimin dhe lehtësimin e jetës së qytetarëve.

Me përdorimin e IA-së në sferën e shëndetësisë mund të përmirësohet mbrojtja shëndetësore (shembull: vendosja e diagnozës më precize dhe më të shpejtë të pacientëve, mundësimi i parandalimit të sëmundjeve të ndryshme që pacientët të shmangin sëmundje të mëtejme etj). IA-ja mund të aplikohet edhe për realizim më të shpejtë, më të thjeshtë dhe më cilësor të të drejtave të mbrojtjes sociale (shembull: shtesë fëmijërore për arsim – studim, shfrytëzim të së drejtës së shtesës prindërore për fëmijë etj.), për ndarje të bursave, subvencioneve, rritje të efikasitetit të bujqësisë, kontributi dhe adaptimi i ndryshimeve klimatike, përmirësimi i sistemeve prodhuese (përmes rritjes së sigurisë së qytetarëve), e me qëllim dhe në drejtim të ruajtjes ose avancimit të cilësisë së jetës së qytetarëve.

13 Burimi: Wikipedia - ChatGPT

Krahas përfitimeve të lartpërmendura të cilat në vetvete i bart IA-ja, ajo sjell edhe rreziqe potenciale të cilat mund të jenë në formë të ndryshme.

Sistemet e IA-së mund të shpijnë në diskriminim dhe të shkaktojnë pabarazi ndërmjet qytetarëve. Deri te diskriminimi mund të arrihet sepse të dhënat që përdoren për t'i ndihmuar IA-së që të sjellë vendime, tashmë në vetvete përmbajnë anshmëri (diskriminim në bazë të gjinisë, ngjyrës së lëkurës, kombësisë, fesë, etj.).

Krahas kësaj, IA-ja mund të hakohet ose manipulohet, gjë që pashmangshmërisht do të rezultojë me dëm të konsiderueshëm të të drejtave dhe lirive të qytetarëve. Rrezik tjetër mund të jetë edhe varësia nga IA-ja për sjellje të vendimeve të rëndësishme. Megjithëse IA-ja mund të ndihmojë të automatizohen proceset dhe të identifikohen problemet, ajo nuk e zëvendëson gjykimin njerëzor.

Aplikimi i gabuar i IA-së mund t'i rrezikojë dukshëm të drejtat e qytetarëve, jo vetëm si të tilla, por edhe në mënyrën e realizimit dhe praktikimit.

IA-ja në fakt mund të ndikojë negativisht mbi gamën e gjerë të të drejtave tona të njeriut. Problemi plotësohet me faktin që vendimet miratohen në bazë të këtyre sistemeve, e njëkohësisht nuk ekziston transparencë, llogaridhënie dhe masa mbrojtëse për atë se si ato janë dizajnuar, si funksionojnë dhe si mund të ndryshohen me kalimin e kohës.

Vendimet e miratuara pa u analizuar rezultatet nga algoritmi i gabuar mund të kenë pasoja serioze për njeriun. Për shembull, personat me aftësi të kufizuara që kanë të drejtën e përfitimeve nga sfera e mbrojtjes shëndetësore janë të refuzuara gabimisht nga softueri dhe të njëjtët më tutje janë përballuar me pasojat nga vendimi i tillë. IA-ja ka potencial për t'u ndihmuar njerëzve që ta shfrytëzojnë maksimalisht kohën, lirisë dhe fatin. Me ç'rast, është shumë vështirë, e me atë edhe e domosdoshme që të gjendet një baraspeshë e vërtetë ndërmjet zhvillimit teknologjik dhe mbrojtjes së të drejtave të njeriut.

Të gjitha organizatat pa marrë parasysh nëse bëhet fjalë për organ shtetëror ose kompani private, duhet të posedojnë IA ekspertizë që Akti i IA-së të funksionojë në mënyrë efektive. Akti i IA-së nuk do të funksionojë dhe do të bëjë dëm të konsiderueshëm nëse institucionet nuk kanë ekspertizë të mjaftueshme për atë si t'i testojnë sistemet e IA-së, si ta vlerësojnë ndikimin e tyre ndaj shoqërisë dhe si të menaxhojnë me to në mënyrë efektive.

9.3.1 Vlerësimi i ndikimit mbi të drejtat e njeriut të sistemeve të IA-së

Një prej detyrimeve themelore ndërkombëtare dhe kushtetuese është mbrojtja e të drejtave të njeriut, e cila duhet të merret parasysh nga institucionet publike gjatë prokurimit të sistemeve të IA-së ose sistemeve të menaxhuara nga algoritmi.

Para se të dizajnohet, zhvillohet ose implementohet cilido sistem i IA-së, nevojitet të realizohet Vlerësim i ndikimit mbi të drejtat e njeriut të sistemeve të IA-së, për

faktin që sistemet e IA-së do të kenë ndikim negativ potencial mbi të drejtat e njeriut dhe ato mund të përbëjnë kërcënim për mjedisin jetësor, jetën e njeriut, demokracinë dhe sundimin e ligjit.

Vlerësimi i ndikimit mbi të drejtat e njeriut luan rol kryesor në mbrojtjen e të drejtave të njeriut dhe është me rëndësi esenciale për sigurimin e besimit të publikut në teknologjinë lidhur me IA-në. Që të fitohet besimi në sistemet e IA-së, vlerësimet e ndikimit duhet të jenë praktikë e detyrueshme ku të drejtat e njeriut do të shqyrtohen në mënyrë adekuate dhe do të respektohen në mënyrë të plotë. Pavarësisht metodologjisë së miratuar, procesi i vlerësimit doemos duhet të jetë transparent, i përgjegjshëm, participativ dhe i inkorporuar në kontekstin më të gjerë shoqëror mbi të cilin mund të ketë ndikim teknologjia.

Në vazhdim propozojmë kornizë të treguesve[14] që kanë për qëllim sigurimin e udhëzimeve për vlerësimin e ndikimit gjatë prokurimit të sistemeve të IA-së të cilat do të sigurojnë mbrojtje të të drejtave të njeriut. Duke i ndjekur treguesit, institucioneve shtetërore dhe programuesve u ofrohet fleksibilitet të mjaftueshëm për ta përshtatur procesin e vlerësimit dhe njëkohësisht të vërtetojnë nëse metodat e tyre janë adekuate që të bëhet vlerësim i saktë dhe të zbutet ndikimi mbi të drejtat e njeriut.

- *Treguesi 1: Korniza normative*

Ky tregues mat nëse procesi i vlerësimit është bazuar në standardet juridike ndërkombëtare relevante lidhur me të drejtat e njeriut. Qëllimi i tij është, gjithashtu, të sigurohet nëse vëllimi dhe përmbajtja e vlerësimit mundëson identifikim të saktë dhe zbutje të ndikimeve negative mbi të drejtat e njeriut, përfshirë edhe gjendjet ku ndikimet negative mbi të drejtat e njeriut janë goxha të larta dhe e pamundur të zbuten.

- *Treguesi 2: Procesi transparent dhe i përgjegjshëm i vlerësimit*

Ky tregues mat nëse vlerësimet e ndikimit janë transparente, llogaridhënëse dhe përsëritëse (të inkorporuara në ciklin e jetës të sistemeve të IA-së). Gjithashtu, mat nëse është e qartë ndarja e roleve dhe përgjegjësive ndërmjet institucioneve publike dhe furnizuesve si dhe ndërmjet të punësuarve te të dyja palët që të parandalohet dispersioni i llogaridhënies. Ky tregues e mat nivelin e transparencës së proceseve për prokurim dhe vlerësim të ndikimit, përfshirë edhe informatat që duhet të zbulohen nga furnizuesi/përgjegjësi për zhvillimin e softuerit të institucionit shtetëror.

- *Treguesi 3. Metodologjia për vlerësimin e ndikimit*

Ky tregues mat nëse metodologjia për vlerësimin e ndikimit të të drejtave të

14 *Burimi: Draft indicators for human rights impact assessment of IT services/products in procurement processes by European Center for Not-for-Profit Law prepared for the needs of the project "Privacy by Design – Building an Inclusive Digital Ecosystem", supported by the EU and implemented by Metamorphosis Foundation and Association Konekt.*

njeriut garanton pasqyrë të rëndësishme dhe përgjegjëse të ndikimeve të sistemit të IA-së. Kjo pjesë nuk imponon metodë specifike për vlerësim, por përmban listë të pyetjeve që të vlerësohet nëse metodologjia e zgjedhur është adekuate, efektive dhe e saktë që të sigurohet harmonizimi me të drejtat e njeriut.

- *Treguesi 4: Angazhimi i rëndësishëm i palëve të interesuara*

Ky tregues mat nëse palët e interesuara relevante (individët dhe grupet e interesuara, organizatat civile, sindikatat, institucionet kombëtare për të drejtat e njeriut, , shoqatat industriale, ekspertët për të drejtat e njeriut, ekspertët akademikë etj) janë angazhuar për përcaktimin e ndikimeve (potenciale) të sistemit të IA-së. Angazhimi i tillë është me qëllim të identifikimit të rreziqeve si dhe masave për zbutje të tyre, e me atë të ndërtohet edhe besimi i publikut në teknologjinë.

- *Treguesi 5. Mbikëqyrja dhe monitorimi efektiv*

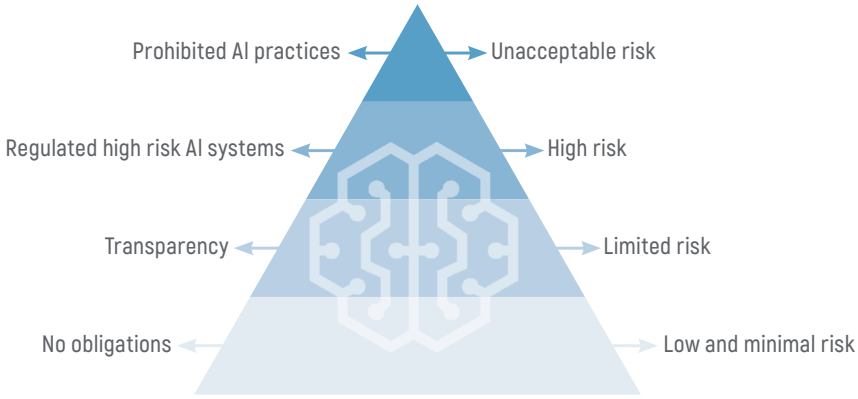
Ky tregues mat nëse vlerësimi i ndikimit është llogaridhënës para mbikëqyrjes/revizorit të jashtëm dhe nëse është objekt i kontrollorit publik. Qëllimi i këtij treguesi është garantimi i kornizës institucionale për monitorim dhe vlerësim të vazhdueshëm në rast nëse ka ndryshim në kontekstin dhe paraqitje të ndikimeve të reja mbi të drejtat e njeriut.

9.4 Rreziqet në përputhje me Aktin evropian për inteligjencë artificiale[15]

Akti në vetvete parasheh qasje të bazuar në rreziqe ndaj sistemeve të cilat mund jenë:

- Sistem me rrezik të papranueshëm;
- Sistem me rrezik të lartë;
- Sistem me rrezik të kufizuar;
- Sistem me rrezik të ulët ose minimal.

15 Burimi: EPRS | European Parliamentary Research Service: Briefing, EU Legislation in Progress (Artificial intelligence act



Data Source: European Commission.

Figura 1. Burimi: Komisioni Evropian: Nivele të klasifikuara të rrezikut

Koncepti i "sistemit të bazuar në IA me rrezik të lartë" nuk është përkufizuar në mënyrë eksplicite. Në vend të kësaj, një grup i sistemeve të inteligjencës artificiale janë klasifikuar si të tilla me kusht që të përmbushen kushtet e caktuara.

Akti nuk ofron përkufizim të përcaktuar për "sistemin e IA-së me rrezik të lartë", por i klasifikon përdorimet specifike të IA-së si me rrezik të lartë dhe ato janë cekur në Shtojcën nr. 5 të kësaj Metodologjie.

Shtojca nr. 5, si pjesë e Aktit i paraqet hollësisht sistemet me rrezik të lartë për IA, mund të ndryshohet nga Komisioni Evropian sipas kushteve të caktuara të cekura në Aktin. Akti për IA doemos duhet të përcaktojë standarde të përcaktuara qartazi dhe juridikisht për zbatim nëse legjislacioni hyn në fuqi. Legjislacioni doemos duhet të mbështesë proces objektiv që të caktohet se cilat sisteme janë "me rrezik të lartë" dhe ta mënjanojë çdo "shtresë plotësuese" të shtuar në procesin për klasifikim të rrezikut të lartë. Shtresa e tillë do t'u lejojë personave përgjegjës për zhvillim të IA-së pa përgjegjësi ose mbikëqyrje për të vendosur nëse sistemet e tyre përbëjnë "rrezik mjaft të konsiderueshëm" që të garantohet kontrolli juridik sipas rregullativës.

Procesi i tillë i klasifikimit të rreziqeve sjell rrezik për dëmtimin e gjithë Aktit të IA-së, përkatësisht vendosjen e sfidave të patejkalueshme për zbatim dhe harmonizim dhe nxitje të kompanive më të mëdha për t'i klasifikuar sistemet e tyre të IA-së me nivel më të ulët të rrezikut.

Në përputhje me Aktin e lartpërmendur do të:

- fusë pasiguri të lartë juridike për atë se cilat sisteme konsiderohen me "rrezik të lartë";
- shpjerë në fragmentimin e tregut të vetëm të BE-së, me interpretime të ndryshme për atë se çfarë përbën "rrezik të lartë" në vendet anëtare;

- rezultojë me atë se autoritetet e vendeve anëtare do të përballohen me sfida serioze për zbatim të legjislacionit, pa resurse të mjaftueshme për monitorim të mjaftueshme të vetëvlerësimit të programuesve;
- lejojë që programuesit t'i shmangin kërkesat themelore të ligjit që kanë për qëllim t'i bëjnë sistemet e tyre më të sigurta. Kjo do t'i lë në pozitë të pavolitshme zhvilluesit përgjegjës të IA-së.
- Pyetja lidhur me atë se cilat sisteme të IA-së duhet të ndalohen (dhe si të përcaktohen këto sisteme në mënyrë precize) dhe çfarë lloje sistemesh të IA-së duhet të klasifikohen si rrezik i lartë mbetet temë e debatit aktual, si dhe kritika nga qarkullimi i propozimit të parë të Komisionit Evropian.

- **Rrezik i papranueshëm: Praktika të ndaluara të inteligjencës artificiale**

Sipas Kapitullit 2, neni 5 i Aktit, këto sisteme të IA-së janë ndaluar për përdorim, sepse ato krijojnë rrezik të papranueshëm që përbën kërcënim për sigurinë, shëndetin, ekzistencën dhe të drejtat e njerëzve. Këto janë sisteme të cilat përdorin "teknika subliminale, përkatësisht teknika të cilat mund të jenë të rrezikshme për njerëzit" të cilat shkaktojnë shkelje psikologjike të njerëzve, sisteme të inteligjencës artificiale që shfrytëzojnë grupe të caktuara vulnerabile të njerëzve (me aftësi të kufizuar fizike dhe mendore), sisteme të përdorura nga organe shtetërore ose në emër të tyre për vlerësim ose klasifikim të konfidencialitetit të personave fizikë në periudhë të caktuar kohore në bazë të sjelljes së tyre sociale ose sisteme për identifikim biometrik në distancë "në kohë reale" në hapësirat e disponueshme publike për qëllimet e zbatimit të ligjit, përveç në një numër të kufizuar të rasteve të cekura në kapitullin 2, neni 5 i Aktit.

- **Rrezik i lartë: Sistemet e rregulluara të inteligjencës artificiale me rrezik të lartë**

Kapitulli 3, neni 6 i Aktit të propozuar për IA i rregullon sistemet "me rrezik të lartë" të IA-së që ndikojnë mbi shëndetin, sigurinë dhe të drejtat themelore të njeriut. Një sistem konsiderohet me rrezik të lartë kur janë përmbushur kushtet në vijim:

- Sistemet që përdoren si komponentë të sigurisë të prodhimit ose që bëjnë pjesë te shëndeti dhe siguria e legjislacionit të BE-së për harmonizim (p.sh., lodrat, aviacioni, automjetet, mjetet ndihmëse mjekësore, ashensorët).
- Sistemi i inteligjencës artificiale si produkt i nënshtrohet confirmity assesment (në tekstin e mëtutjeshëm të njohur si vlerësim i përputhshmërisë, të sqaruar më hollësisht në pjesën 10 dhe 11), ndërsa nga pala e tretë para se të vihet në tregun e BE-së.

Gjithashtu, sisteme të caktuara për IA janë klasifikuar si me rrezik të lartë dhe këto sisteme janë cekur në (Shtojcën 2 të kësaj Metodologjie) të Aktit për inteligjencë artificiale të BE-së.

Ekzistojnë tetë sisteme kryesore për IA të cilat mund të klasifikohen si me rrezik të lartë dhe atë:

❖ **Identifikimi biometrik i personave fizikë**

- sisteme të inteligjencës artificiale të dedikuara për t'u përdorur për identifikim biometrik në distancë të personave fizikë "në kohë reale dhe joreale".

- **Menaxhimi dhe funksionimi i infrastrukturës kritike**

- Sistemet e IA-së të dedikuara për t'u përdorur si komponentë të sigurisë në menaxhimin dhe funksionimin e komunikacionit rrugor dhe në furnizimin me ujë, gaz, energji të ngrohjes dhe energji elektrike.

- **Arsimi dhe trajnimi profesional**

- Sistemet e IA-së të dedikuara për t'u përdorur me qëllim të caktimit të qasjes ose të emërimit të personave fizikë në institucione arsimore dhe profesionale, sisteme të inteligjencës artificiale të dedikuara për t'u përdorur për qëllimet e vlerësimit të nxënësve në institucionet arsimore dhe trajnime profesionale dhe për vlerësimin e nxënësve në testet të cilët zakonisht nevojiten për pranim në institucionet arsimore (p.sh., pikat e provimeve).

- **Punësimi, menaxhimi me të punësuarit dhe qasja në vetëpunësim**

- Sistemet për inteligjencë artificiale të dedikuara për t'u përdorur për rekrutim ose përzgjedhje të personave fizikë, veçanërisht për shpallje të vendeve të lira të punës, analizë ose filtrim të aplikacioneve për punësim, vlerësim të kandidatëve gjatë intervistave ose testeve si dhe IA e dedikuar për t'u përdorur për sjellje të vendimeve për avancim dhe prishje të marrëdhënieve kontraktuese lidhur me punën, për shpërndarje të detyrave dhe për ndjekje dhe vlerësim të performancave dhe sjelljes së të punësuarve ose personave të angazhuar.

- **Qasja dhe përfitimet nga përdorimi i shërbimeve private dhe publike**

- Sistemet e IA-së të dedikuara për t'u përdorur nga organet shtetërore ose në emër të organeve shtetërore që të vlerësohet përshtatshmëria e personave fizikë për shërbime sociale dhe publike, si dhe për ndarje, zvogëlim, revokim ose kthim të përfitimeve dhe shërbimeve të tilla, sisteme të IA-së të dedikuara për t'u përdorur për vlerësim të aftësisë kreditore të personave fizikë ose për përcaktimin e rejtingut të tyre të kredisë, sisteme të IA-së të dedikuara për t'u përdorur për dërgim ose për përcaktim të prioritetit në dërgimin e shërbimeve për reagim të parë në raste urgjente, përfshirë edhe zjarrfikësit dhe ndihmën mjekësore.

- **Zbatimi i ligjit**

-Sistemet e AI-së të dedikuara për t'u përdorur nga organet e zbatimit të ligjit për përgatitjen e vlerësimeve individuale të rrezikut të personave fizikë në mënyrë që të vlerësohet rreziku që personi fizik të kryejë shkelje në kundërshtim me ligjin ose ta përsërisë veprën ose viktimat potenciale të veprave penale; sistemet e IA-së të dedikuara për t'u përdorur nga organet e zbatimit të ligjit si poligrafi dhe mjete të ngjashme ose për të zbuluar gjendjen emocionale të një personi fizik; Sistemet e IA-së të dedikuara për t'u përdorur nga organet e zbatimit të ligjit për të zbuluar falsifikime të thella siç ceket në nenin 52(3) të Aktit; sistemet e IA-së të dedikuara për t'u përdorur nga organet e zbatimit të ligjit për të vlerësuar besueshmërinë e provave gjatë hetimit ose ndjekjes penale të autorëve të krimeve; Sistemet e IA-së të dedikuara për t'u përdorur nga organet e zbatimit të ligjit për të parashikuar ndodhjen ose përsëritjen e veprës së vërtetë ose potenciale penale bazuar në profilizimin e personave fizikë siç ceket në nenin 3(4) të Direktivës (BE) 2016/680[16] ose vlerësimin e tipareve dhe karakteristikave të personalitetit ose sjelljes kriminale në të kaluarën e personave fizikë ose grupeve të personave fizikë; Sistemet e IA-së të dedikuara për t'u përdorur nga organet e zbatimit të ligjit për të profilizuar personat fizikë siç ceket në nenin 3(4) të Direktivës (BE) 2016/680 gjatë zbulimit, hetimit ose ndjekjes së autorëve të veprave penale; Sistemet e IA-së të dedikuara për t'u përdorur për analitikën e krimit lidhur me personat fizikë, duke u lejuar organeve të zbatimit të ligjit të kërkojnë përmbledhje të mëdha të lidhura dhe të palidhura të ndërlikuara të disponueshme nga burime të ndryshme të të dhënave ose në formate të ndryshme të të dhënave, me qëllim të identifikimit të skemave të panjohura ose të zbulimit të marrëdhënieve të fshehura në të dhënat.

- **Menaxhimi me migrimin, azilin dhe kontrollin kufitar**

Sistemet e IA-së të dedikuara për t'u përdorur nga organet shtetërore kompetente si poligraf dhe mjete të ngjashme ose të zbulohet gjendja emocionale e personit fizik; sistemet e IA-së të dedikua për t'u përdorur nga organet shtetërore kompetente që të vlerësohet rreziku, përfshirë edhe rrezikun e sigurisë, rrezikun e imigrimit joligjor ose rrezikun shëndetësor, që e sjell personi fizik i cili ka për qëllim të hyjë ose ka hyrë në territorin e vendit anëtar të BE-së; sistemet e IA-së të dedikuara për t'u përdorur nga organet shtetërore kompetente për kontroll të autenticitetit të dokumenteve të udhëzimit dhe dokumentacionit shoqërues të personave fizikë dhe zbulim të dokumenteve joautentike me kontroll të karakteristikave të tyre të sigurisë; sistemet e IA-së të dedikuara për t'u ndihmuar organeve shtetërore kompetente për shqyrtim të kërkesave për azil, vizës dhe lejeve të qëndrimit dhe ankesave shoqëruese lidhur me përshtatshmërinë e personave fizikë që aplikojnë.

16 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

- **Zbatimi i të drejtave dhe proceseve demokratike**

- Sistemet për IA të dedikuara për t'u ndihmuar organeve të drejtësisë në hetimin dhe interpretimin e fakteve dhe ligjit dhe gjatë zbatimit të ligjit për grup konkret të fakteve.

Figura 2. Sistemet e klasifikuara të IA-së me rrezik të lartë

Megjithatë, doemos duhet të theksohet se nuk konsiderohet me rrezik të lartë çdo sistem i IA-së në këto kategori. Ekzistojnë qëndrime për secilën prej këtyre fushave, të cilat doemos duhet të analizohen në mënyrë të detajuar që të konstatohet nëse sistemi i dhënë i IA-së vërtet konsiderohet me rrezik të lartë ose jo.

Të gjithë këto sisteme të IA-së me rrezik të lartë do t'i nënshtrohen një grupi të rregullave të reja, përfshirë:

- Kusht për vlerësimin ex-ante të përputhshmërisë: Ofruesit e sistemeve të IA-së me rrezik të lartë do të kërkohet t'i regjistrojnë sistemet e tyre në bazën e të dhënave të BE-së (të menaxhuar nga Komisioni Evropian), para se të lëshohen në treg ose të vihen në përdorim. Të gjitha produktet dhe shërbimet e bazuara në IA të rregulluara me legjislacionin ekzistues për siguri të produkteve do të bëjnë pjesë në kornizën ekzistuese të cilat tashmë aplikohen (p.sh. për mjete ndihmëse mjekësore). Ofruesit e sistemeve të IA-së të cilat momentalisht nuk janë rregulluar nga legjislacioni i BE-së do të duhet të realizojnë vlerësim personal të përputhshmërisë (vetëvlerësim) se janë harmonizuar me kërkesat e reja dhe mund të përdorin shenjën "CE". Vetëm për sistemet e IA-së me rrezik të lartë të cilat përdoren për identifikim biometrik do të kërkohet vlerësim të përputhshmërisë nga "trup i autorizuar".
- Kërkesa tjera: Sistemet e tilla të IA-së me rrezik të lartë duhet të harmonizohen me një sërë kërkesash veçanërisht për menaxhim me rrezik, testim, qëndrueshmëri teknike, trajnim dhe menaxhim me të dhënat, transparencë, mbikëqyrje njerëzore dhe siguri kibernetike (Kapitulli 2, nenet nga 8 deri 15 të Aktit). Në këtë aspekt, ofruesit e shërbimeve, importuesit, shpërndarësit dhe përdoruesit e sistemeve të IA-së me rrezik të lartë do të duhet doemos të përmbushin një sërë detyrimesh. Ofruesit jashtë BE-së do të kërkojnë përfaqësues të autorizuar në BE që (mes tjerash) të realizojnë vlerësim të përputhshmërisë, të vendosin sistem për monitorim pas vënies së tij në funksion dhe sipas nevojës të ndërmerren masa korrigjuese. Sistemet e IA-së të cilat janë në përputhje me standardet e reja të harmonizuara të BE-së, momentalisht në zhvillim e sipër, do të kenë dobi nga supozimi për harmonizim me draft-kërkesat e Aktit.

- **Rrezik i kufizuar: Detyrime për transparencë**

Sistemet e IA-së të cilat janë të klasifikuara si sisteme me "rrezik të kufizuar", siç janë sistemet të cilat komunikojnë me njerëz (përkatësisht çet-bote), sisteme për njohje të emocioneve, sisteme për kategorizim biometrik dhe sisteme të IA-së që gjenerojnë dhe manipulojnë me fotografi, përmbajtje të zërit ose videos (ang. deep fake), do të jenë objekt i një seti të kufizuar të detyrimeve për transparencë. Si për shembull, provajderët sigurojnë informata për sistemet e IA-së të dedikuara për bashkëveprim me personat fizikë të cilat janë të dizajnuara dhe të zhvilluara në atë mënyrë që personat fizikë informohen se kanë bashkëveprim me sistemin e IA-së, përveç nëse kjo nuk është e dukshme nga rrethanat dhe konteksti i përdorimit ose personat fizikë të cilat janë të ekspozuara ndaj sistemit për njohje të emocioneve ose sistemit për kategorizim biometrik janë njoftuar për punën e sistemit.

- **Rrezik i ulët ose minimal: Nuk ka detyrime**

Të gjitha sistemet tjera të IA-së që përbëjnë vetëm rrezik të ulët ose minimal mund të zhvillohen dhe përdoren në BE pa u harmonizuar me çfarëdo detyrime ligjore shtesë. Megjithatë, Akti i propozuar e parasheh krijimin e kodeve të sjelljes që të nxiten provajderët e sistemeve të IA-së me rrezik të ulët t'i aplikojnë vullnetarisht kërkesat për sistemet e IA-së me rrezik të lartë.

9.5 Kërkesat për sisteme të inteligjencës artificiale me rrezik të lartë

Akti i vendos kërkesat për sistemet e IA-së me rrezik të lartë në Kapitullin 2 dhe provajderëve të shërbimeve, si dhe përdoruesve të këtyre sistemeve u imponon në mënyrë sukcesive detyrime.

Ekzistojnë shtatë kërkesa kryesore të parapara sipas neneve nga 9 deri 15 të Aktit të cilat duhet t'i plotësojnë sistemet e IA-së, që të konsiderohen konfidencialë, dhe atë:

1. Sistemi për menaxhim me rrezikun;
2. Menaxhimi me të dhënat;
3. Dokumentacioni teknik;
4. Mbajtja e evidencës;
5. Transparenca dhe dhënia e informatave përdoruesve;
6. Mbikëqyrja njerëzore;
7. Saktësia, rezistenca dhe siguria kibernetike.

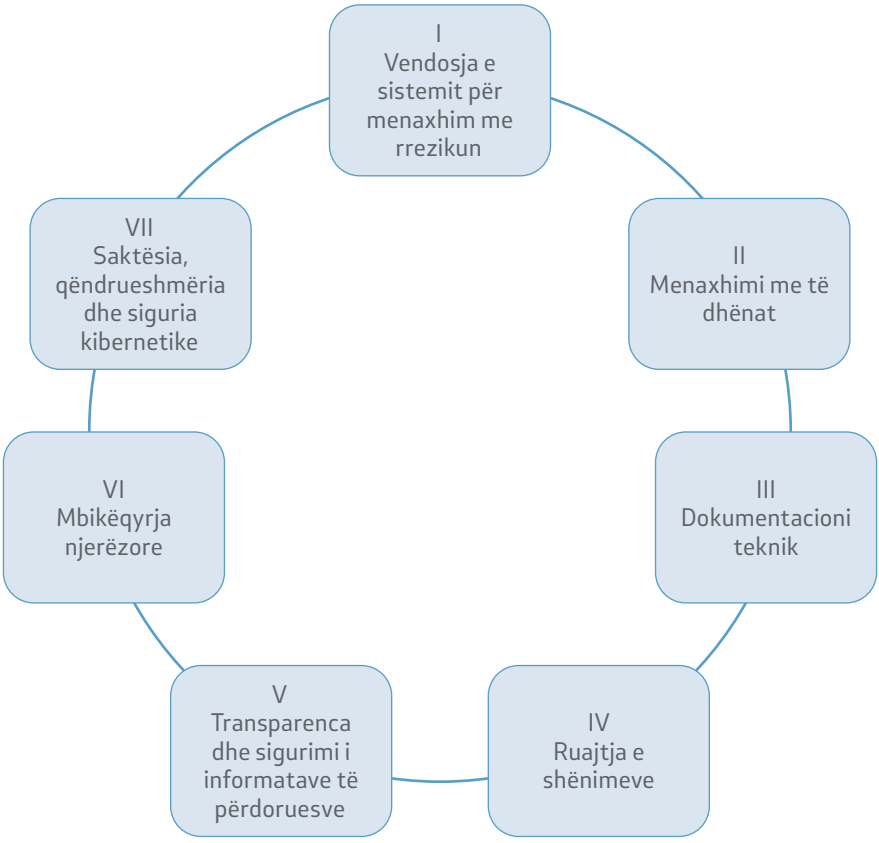


Figura 3 . Kërkesa për sistemet e inteligjencës artificiale me rrezik të lartë

Përputhshmëria me këto kërkesa është e detyrueshme për entitetet e përfshira. Megjithatë, niveli i harmonizimit do të përcaktohet duke e marrë parasysh "state of the art" në përputhje me nenin 8, alineja 1 e ligjit. Gjithashtu, harmonizimi me këto kërkesa mund të kërkojë marrjen parasysh të dispozitave për çështje të tjera kontestuese, përfshirë, por pa u kufizuar në, përgjegjësinë për produktin, mbrojtjen e të dhënave, të drejtat e autorit, pronësinë intelektuale dhe sekretet afariste. Me ç'rast, harmonizimi i duhur do të kërkojë një analizë të detajuar dhe shumështresore e cila është e përshtatur me specifikat e secilit sistem për IA.

E rëndësishme është se shumica e këtyre kërkesave duhet doemos të përfshihen në dizajnin e sistemit për IA me rrezik të lartë. Përveç dokumentacionit teknik të cilin duhet ta përgatitë provajderi, kërkesat tjera duhet të merren parasysh që në fazat më të hershme të dizajnimit dhe zhvillimit të sistemit për IA. Edhe nëse provajderi nuk është dizajnues/zhvillues i sistemit, ata megjithatë duhet të kujdesen që kërkesat e atij Kapitulli të përfshihen në sistem për të arritur harmonizim.

9.6 Trupi mbikëqyrës

Vendet anëtare kërkojnë të caktohen organe "kompetente" ose "të autorizuara", të cilët do të kenë për detyrë ta mbikëqyrin implementimin dhe harmonizimin me rregullativën e sistemeve të IA-së. Organet mbikëqyrëse do të jenë përgjegjëse për vlerësimin e harmonizimit të provajderëve me detyrimet dhe kërkesat për sistemet e IA-së me rrezik të lartë. Ato do të kenë qasje në informatat konfidenciale (përfshirë kodin burimor të sistemeve të IA-së) dhe do të obligohen me sigurimin e atij konfidencialitet.

Gjithashtu, prej tyre do të kërkohet të ndërmerren çfarëdo masash korrigjuese për ndalim, kufizim, tërheqje ose revokim të sistemeve të IA-së të cilat nuk janë në pajtim me Aktin ose të cilat, megjithëse janë të harmonizuara, përbëjnë rrezik për shëndetin ose sigurinë e njerëzve dhe mbrojtjen e të drejtave të tyre. Në rast të mosharmonizimit të vazhdueshëm, vendet anëtare do të duhet doemos të ndërmarrin masa adekuate për kufizim, ndalim, revokim ose tërheqje nga tregu të sistemit të IA-së me rrezik të lartë.

10. VLERËSIM I PËRPUTHSHMËRISË (ANG. CONFORMITY ASSESSMENT)

Detyrim kryesor të cilin e imponojnë sistemet e IA-së me rrezik të lartë është vlerësimi i përputhshmërisë të cilin provajderët e sistemeve të tilla duhet ta realizojnë para se t'i plasojnë në treg.

Vlerësimi i përputhshmërisë është detyrim ligjor i dizajnuar për ta nxitur përgjegjësinë e cila ka të bëjë vetëm me sistemet e IA-së të klasifikuara si "me rrezik të lartë".

Gjithashtu, vlerësim i ri i përputhshmërisë duhet të bëhet kur sistemi për IA me rrezik të lartë është ndryshuar thelbësisht ose rezulton me modifikim të dedikuar për sistemin e IA-së.

Ky proces duhet të zbatohet nga provajderi i sistemit me rrezik të lartë, por gjithashtu, në situata specifike mund të zbatohet edhe nga prodhuesi, shpërndarësi, si dhe nga pala e tretë.

Vlerësimi specifik i përputhshmërisë, dhe i cili duhet të realizohet për sisteme të IA-së me rrezik të lartë, varet nga kategoria dhe lloji i inteligjencës artificiale e cila është në pyetje.

Akti parasheh dy lloje të ndryshme të vlerësimit të përputhshmërisë varësisht nga lloji i sistemit me rrezik të lartë për IA dhe atë:

❖ Vlerësimi i brendshëm

Ky vlerësim nuk kërkon përfshirje të palës së tretë të pavarur. Provajderi/ prodhuesi i sistemit të IA-së/pala tjetër doemos duhet:

- Të vërtetojë se ka sistem të implementuar për menaxhim me cilësinë i cili përfshin shumë karakteristika, përfshirë edhe menaxhimin me rrezik, procedurën për paraqitjen e incidenteve (p.sh. cenimi i sigurisë së të dhënave, defekt i sistemit dhe identifikimi i rreziqeve të cilat nuk kanë qenë të dukshme më parë) dhe procedurat për testim dhe vlefshmëri për menaxhim me të dhënat.
- T'i ketë analizuar informatat në dokumentacionin teknik të sistemit të IA-së, që ta vlerësojë harmonizimin e sistemit të IA-së me kërkesat esenciale relevante për sisteme të IA-së me rrezik të lartë sipas rregullativës së propozuar.
- Të vërtetojë se procesi i dizajnimit dhe zhvillimit të sistemit të IA-së dhe monitorimi i tij pas plasimit në treg që është cekur në nenin 61 është në përputhje me dokumentacionin teknik të sistemit (ky dokumentacion përfshin informata për aftësitë e sistemit të IA-së dhe për kufizim të sistemit, algoritme të përdorura, të dhëna, trajnime, testim dhe procese të vlefshmërisë).
- Pasi entiteti përgjegjës ta realizojë vlerësimin e brendshëm të përputhshmërisë, ai duhet të përgatisë deklaratë me shkrim për harmonizim, për çdo sistem të IA-së.

Shenja "CE" për Vlerësim të përputhshmërisë, duhet të jetë e dukshme, e lexueshme dhe e pashlyeshme për të gjitha sistemet e IA-së me rrezik të lartë. Atje ku nuk është e mundshme ose nuk është e arsyetuar për shkak të natyrës së sistemit të IA-së me rrezik të lartë, ajo vihet në dokumentacionin shoqërues, siç është e përshtatshme.

❖ Vlerësimi nga pala e tretë (trupi i autorizuar)

Këtë vlerësim e realizon pala e tretë e cila do të lëshojë certifikatë për vërtetim të harmonizimit të sistemit për IA.

Nga provajderi do të kërkohet të dorëzohet dokumentacion dhe informata lidhur me sistemin për menaxhim me cilësinë dhe dokumentacionin teknik, sipas procesit të sqaruar në Shtojcën 7 të kësaj Metodologjie, dhe trupi i autorizuar do t'i përdorë dokumentacionin dhe informatat që të konstatojë nëse sistemi i IA-së i përmbush kërkesat relevante.

Krahas kësaj, rregullativa e propozuar do të kërkojë nga provajderi t'i lejojë trupit të autorizuar të qaset në hapësirat ku bëhet dizajni, zhvillimi dhe testimi i sistemeve të IA-së, të bëjë "revizione periodike" që të sigurohet se provajderi i mirëmban dhe

i aplikon sistemet për menaxhim me cilësinë dhe, atje ku ekziston domosdoshmëri racionale që të vlerësohet përputhshmëria, të ketë qasje në kodin burimor të sistemit të IA-së.

Nëse trupi i autorizuar konstaton se sistemi i IA-së me rrezik të lartë është në përputhje me kërkesat, ai do të lëshojë certifikatë për vlerësimin e dokumentacionit teknik i cili ka vlefshmëri të kufizuar kohore dhe mund të suspendohet ose tërhiqet nga trupi i autorizuar. Ngjashëm me vlerësimin e brendshëm të përputhshmërisë, procesin e vlerësimit të përputhshmërisë të kryer nga pala e tretë, provajderi duhet ta përgatisë formularin për deklaratë – që përmban, mes tjerash, përshkrim të procedurës së zbatuar për vlerësim të përputhshmërisë.

Në rast se trupi i autorizuar vlerëson se sistemi i IA-së me rrezik të lartë nuk është në përputhje me kërkesat për sisteme të IA-së me rrezik të lartë, ai duhet ta njoftojë dhe t'ia sqarojë në mënyrë të detajuar provajderit ose entitetit tjetër përgjegjës. Provajderi (ose entitet tjetër përgjegjës) ka të drejtë të ankesës kundër vendimit të trupit të autorizuar. Në këtë rast, provajderi/entiteti përgjegjës doemos duhet t'i ndërmarrë aktivitetet e nevojshme korrigjuese. Këto aktivitete mund të lëvizin nga procesi i harmonizimit me kërkesat, deri te sistemi i tregut.

Sistemet e IA-së me rrezik të lartë doemos duhet t'u nënshtrohen vlerësimeve të reja gjithmonë kur janë "ndryshuar në mënyrë thelbësore", pa marrë parasysh nëse sistemi i ndryshuar do të vazhdojë të përdoret nga përdoruesi aktual ose është dedikuar të shpërndahet më gjerësisht. Sidoqoftë, nevojitet vlerësim i ri nga trupi i autorizuar në çdo 5 minuta, pa marrë parasysh nëse sistemi është ndryshuar ose jo.

11. VLERËSIMI I PËRPUTHSHMËRISË VS VNMDHP

Kjo pjesë në mënyrë krahasuese e analizon vlerësimin e propozuar të përputhshmërisë dhe VNMDHP-në. Megjithëse të dyja detyrimet kërkojnë të bëhet vlerësim i aktiviteteve për përpunim të të dhënave personale me rrezik të lartë (në rast të VNMDHP) dhe sistemeve të IA-së (në rastin e vlerësimit të përputhshmërisë), ekzistojnë edhe dallime edhe karakteristika të përbashkëta të cilat duhet të theksohen.

Sipas LMDHP-së dhe Rregullores për procesin e vlerësimit të ndikimit të mbrojtjes së të dhënave personale, kontrollori është aktori i cili i cakton qëllimet dhe mënyrat e përpunimit të të dhënave personale. Kontrollori është përgjegjës për harmonizim me Ligjin dhe Rregulloren, për vlerësim nëse do të kryhet VNMDHP-ja dhe për kryerje të cilësdo VNMDHP. Sipas Aktit, vlerësimi i përputhshmërisë parimisht realizohet nga provajderi i sistemit të IA-së me rrezik të lartë (ose nga prodhuesi i produktit, shpërndarësi ose importuesi ose personi i tretë, kur janë përmbushur kushtet e veçanta).

Gjatë realizimit të VNMDHP-së, kontrollori duhet t'i identifikojë kërcënimet ndaj të drejtave dhe lirive të personave fizikë, t'i vlerësojë rreziqet lidhur me seriozitetin dhe probabilitetin që ato të materializohen dhe përfundimisht të vendosë për masat e duhura të cilat do t'i zbusin rreziqet e larta. Në të kundërtën, vlerësimi i përputhshmërisë kërkon analizë nëse sistemi i IA-së me rrezik të lartë i përmbush kërkesat specifike të përcaktuara me Aktin, por të cekura më lart në dokumentin. Në listën e llojeve të operacioneve të përpunimit për të cilat kërkohet VNMDHP janë përfshirë operacione për përpunim të cilat mund të lidhen me sistem të IA-së, siç janë për shembull: "përpunimi i të dhënave personale për profilizim sistematik dhe gjithëpërfshirës ose vendimmarrje të automatizuar për të nxjerrë përfundime dhe për të marrë vendime që prodhojnë efekt juridik, të cilat në masë të madhe ndikojnë mbi personin fizik dhe/ose mbi më shumë persona ose që ndihmojnë gjatë marrjes së vendimeve për qasje në shërbim ose në ndonjë lloj të shërbimit ose ndonjë volitshmëri", "përpunimi i kategorive të veçanta të të dhënave personale me qëllim të profilizimit ose vendimmarrjes automatike" ose "përpunimi i të dhënave personale të fëmijëve me qëllim të profilizimit, vendimmarrjes automatike ose për qëllime marketingu ose për ofrimin e drejtpërdrejtë të shërbimeve të dedikuara për ta".

Akti nga ana tjetër përcakton se cilat sisteme të IA-së kualifikohen si "me rrezik të lartë" dhe prandaj kërkon të realizohet vlerësim i përputhshmërisë. Nuk i lihet të drejtës diskrecionale të subjektit përgjegjës për të vlerësuar nëse nevojitet të realizohet vlerësim i përputhshmërisë. Që të realizohet vlerësimi i përputhshmërisë nuk është e rëndësishme që të përpunohen të dhënat personale, megjithëse ato mund të përpunohen si pjesë e përdorimit të sistemit të IA-së. Mjafton që sistemi i IA-së të bëjë pjesë në kornizën e Aktit dhe të kualifikohet si "me rrezik të lartë".

Për realizimin e VNMDHP-së, kontrollori doemos duhet ta vlerësojë "aktivitetin për përpunim" lidhur me rreziqet që i sjell për të drejtat dhe liritë e personave fizikë. Më konkretisht, kontrollori doemos duhet ta shqyrtojë natyrën, fushëveprimin, kontekstin dhe qëllimet e përpunimit, si dhe domosdoshmërinë dhe proporcionalitetin me qëllimin e cekur.

Për realizimin e vlerësimit të përputhshmërisë, provajderi doemos duhet të vlerësojë nëse sistemi ose produkti është dizajnuar dhe zhvilluar në përputhje me kërkesat specifike të Aktit të dedikuara për sistemet e IA-së me rrezik të lartë.

Sipas LMDHP-së kontrollori është ai i cili i cakton qëllimet dhe mjetet për përpunim të të dhënave personale dhe ai konstaton nëse duhet të kryhet VNMDHP.

Ndërsa sipas Aktit të IA-së, vlerësimi i përputhshmërisë parimisht realizohet nga provajderi i sistemit të IA-së me rrezik të lartë (ose nga prodhuesi i produktit, shpërndarësi ose importuesi ose personi i tretë, kur janë përmbushur të dhënat personale.

Detyrimet për realizim të VNMDHP-së dhe vlerësimit të përputhshmërisë janë të ndryshme sipas vëllimit, përmbajtjes dhe qëllimeve. Në disa sfera ato janë të lidhura dhe mund bile edhe të përputhen veçanërisht kur sistemet e IA-së me rrezik të lartë përfshijnë përpunim të të dhënave personale.

Sistemet e IA-së me rrezik të lartë që përfshijnë përpunim të të dhënave personale mund të plotësohen ose të fitojnë mbështetje nga kontrollorët që realizojnë VNMDHP. Detyrimi i Aktit dhe realizimi i vlerësimit të përputhshmërisë mund ta plotësojë boshllëkun lidhur me përgjegjësitë e provajderëve dhe kontrollorëve që i përdorin këto sisteme për përpunim të të dhënave personale. Megjithatë, nëse entiteti është edhe provajder edhe kontrollor në lidhje me sistemin e IA-së që do të përpunojë të dhëna personale, atëherë ai entitet do të kryejë edhe VNMDHP dhe vlerësim të përputhshmërisë.

Qëllimi i fundit i VNMDHP-së është t'i thërrasë kontrollorët e përgjegjësisë për procedurat e tyre dhe të garantojë mbrojtje më efikase të të drejtave të subjekteve. Qëllimi i vlerësimit të përputhshmërisë nga ana tjetër është të garantojë harmonizim me kërkesa të caktuara që janë të krijuara nga masa për zbutje të sistemeve të cilët në vetvete sjellin rreziqe të larta.

12. SHTOJCA NR.1

RAPORTI PËR VNMDHP

(Ekzemplar i plotësuar)

Të dhënat për kontrollorin

Emërtimi i kontrollorit	*Institucioni X*
Oficeri për mbrojtje të të dhënave personale	*Emri dhe mbiemri*
Lënda/Emërtimi i VNMDHP-së	*Aplikacioni për vendimmarrje automatike për ndarje të bursave*

Faza 1: Pyetësori kualifikues

Përgjigjuni me PO ose JO në pyetjen bashkëngjitur.	Po	Jo
1. A mblidhen, përdoren, ruhen ose ndahen çfarëdo të dhëna personale të kategorisë së veçantë gjatë kryerjes së aktivitetit?		Jo
2. A përdoren të dhëna personale gjatë kryerjes së aktivitetit që të parashohin disa preferenca personale, lokacion, lëvizje, gjendje financiare, performancë shëndetësore ose të punës të personave fizikë?		Jo
3. A përpunohen të dhënat personale gjatë kryerjes së aktivitetit lidhur me dënimet ndëshkimore dhe veprat ndëshkimore ose përgjegjësinë për kundërvajtje?		Jo
4. A mundësohet me aktivitetin marrja e vendimeve të cilat mund të ndikojnë dukshëm mbi personat fizikë?	*Po*	
5. A parasheh aktiviteti përdorim të teknologjive të reja ose zgjidhjeve teknologjike ose me mundësi për përpunimin e të dhënave personale që shërbejnë për analizim ose parashikim të gjendjes ekonomike, shëndetit, dëshirave ose interesave personale, sigurimit ose sjelljes, lokacionit ose lëvizjes së personave fizikë?		*Jo*
6. A nënkupton aktiviteti përpunim të të dhënave personale të mbledhura nga palët (personat) e tretë të cilët merren parasysh për vendimmarrje lidhur me lidhjen, zgjidhjen, refuzimin ose vazhdimin e kontratave për ofrim të shërbimeve të personave fizikë?		*Jo*

7. A nënkupton aktiviteti përpunim të të dhënave përmes lidhjes, krahasimit ose kryerjes së kontrollit të ngjashmërive nga më shumë burime?		*Jo*
8. A përfshin aktiviteti monitorim të lokacionit ose të sjelljes së personit fizik të përpunimit sistematik të të dhënave për komunikim (meta të dhëna) të krijuara – të gjeneruara me përdorim të telefonit, internetit ose mjeteve tjera (kanaleve) për komunikim, siç janë GSM, GPS, Wi-Fi, për monitorim dhe përpunim të të dhënave për lokacionin?		Jo
9. A nënkupton aktiviteti përpunim të të dhënave personale përmes përdorimit të pajisjeve dhe teknologjive, te të cilat nëse ndodh incident mund ta rrezikojë shëndetin e një ose më shumë personave?		Jo
10. A bëhet me aktivitetin njëfarë monitorimi sistematik të sipërfaqeve publike në masë të madhe?		Jo
11. A ekzistojnë disa rreziqe tjera lidhur me përdorimin e produktit/shërbimit tuaj për të drejtat dhe liritë e personave fizikë?	*Po*	
12. A nënkupton aktiviteti monitorim ose ndjekje të personave të punësuar?		*Jo*

Faza 2: Përpunimi i të dhënave personale

Përshkrimi i natyrës së përpunimit: Si do të mblidhen, përdoren, ruhen dhe fshihen të dhënat personale? Cili është burimi prej të cilit do të merren të dhënat personale? A do të ndahen të dhënat personale me palët e treta ("pala e tretë" – është secili person fizik ose juridik, organ i pushtetit shtetëror, organ shtetëror ose person juridik i themeluar nga shteti për kryerje të autorizimeve publike, agjencia ose trup tjetër, i cili nuk është subjekt i të dhënave personale, kontrollori, përpunuesi ose personi, i cili nën autorizimin e drejtpërdrejtë të kontrollorit ose përpunuesit është i autorizuar t'i përpunojë të dhënat.

I mbledhim të dhënat në mënyrat në vijim:

- *Me bashkëveprim të drejtpërdrejtë me përdoruesit kur aplikojnë për bursë;*
- *Me përdorim të teknologjive të automatizuara kur përdoruesit e përdorin ueb aplikacionin.*

Kryesisht i përdorim të dhënat personale që të kontrollojmë nëse personi i përmbush kushtet për marrje të bursës. Gjithashtu, të dhënat i përdorim që t'i njoftojmë subjektet të cilët tashmë janë regjistruar për thirrje tjera të hapura për ndarje të bursës.

I përdorim të dhënat që t'i përmbushim qëllimet në vijim:

- *Krijimi i profilit të përdoruesit;*
- *Menaxhimi me relacionet me subjektet (p.sh. Përgjigje të pyetjeve, ankesa dhe ngjashëm);*
- *Për administrim dhe mbrojtje të ueb aplikacionit (p.sh. Mirëmbajtje dhe mbështetje të aplikacionit, zgjidhje të problemeve, hostim dhe ngjashëm);*
- *Për verifikim të identitetit të përdoruesit dhe ofrim të platformës së sigurt;*
- *Për harmonizim me detyrimet rregullatore dhe juridike.*

Skedarë (kukis)

Ueb aplikacioni ynë përdor skedarë për qëllimet në vijim:

Përdorim skedarë të domosdoshme, të cilat nuk janë objekt i kërkesës së pëlqimit, për qëllimet në vijim:

- *Autentifikimi i llogarisë së përdoruesit;*
- *Siguria dhe parandalimi i mashtrimeve;*
- *Balancimi i ngarkimit të faqes së internetit (lord balancing);*

Preferencat për skedarë për mjetin për pëlqim për përdorim të skedarëve

Të dhënat të cilat do të përpunohen:

- *- të dhënat për identitetin: emri, mbiemri, emri i përdoruesit, datëlindja;*
- *- të dhënat për kontakt: adresa, email adresa, numri i telefonit;*
- *- të dhënat financiare: të dhënat për të ardhurat mujore të punëtorëve/ kujdestarëve për 3 (muajt) e fundit;*
- *- të dhënat teknike: IP adresa, të dhënat për hyrje...etj;*

Kategoria e veçantë e të dhënave personale: *Nuk përpunojmë kategori të veçantë të të dhënave personale.*
Sasia e të dhënave personale: *Presim që ueb aplikacioni do të ketë rreth 10.000 përdorues çdo vit.*
Sipërfaqja gjeografike: *Subjektet të dhënat personale të të cilave do të përpunohen janë lokalizuar veçanërisht në Republikën e Maqedonisë së Veriut. Ueb aplikacioni është hostuar në Republikën e Maqedonisë së Veriut.*

Përshkruani kontekstin e përpunimit:

- Cila është natyra e raportit ndërmjet institucionit dhe personave fizikë?
- Sa kontroll do të kishin pasur personat fizikë?
- A do të kishin pritur ato t'ua përpunoni të dhënat personale në këtë mënyrë?
- A përfshin përpunimi përpunimin e të dhënave personale të fëmijëve ose grupeve tjera vulnerabile?
- A ekzistojnë disa shkaqe për shqetësim për këtë lloj të përpunimit ose për lëshime (mangësi) të sigurisë?
- Si është gjendja momentale e teknologjisë e cila do të përdoret?
- A ekzistojnë disa shkaqe për shqetësim të publikut të cilat duhet të merren parasysh?

Në ueb aplikacionin tonë studentët mund të aplikojnë për marrje të bursës. Vetë sistemi pas informatave të marra nga studentët cakton nëse ndonjë student i përmbush/nuk i përmbush kushtet për marrje të bursës. Studentët informohen për mënyrën e tillë të përpunimit në Politikën e privatësisë e cila është e disponueshme gjatë vizitës së këtij ueb aplikacioni. Studentët mund që në çdo moment t'i drejtohen Ministrisë dhe të marrin sqarim për mënyrën në të cilën funksionon algoritmi.....

Përshkruajeni qëllimin e përpunimit:

- Cili është qëllimi i projektit/procesi afarist, cilat janë aktivitetet e parapara të përpunimit të të dhënave personale përkatësisht çfarë dëshirohet të arrihet?
- Cili është ndikimi mbi personat fizikë?
- Cilat janë përfitimet nga përpunimi – për ju, dhe më gjerë?

Qëllimi është të automatizohet dhe të përshpejtohet procesi i ndarjes së bursave. Gjithashtu, qëllimi është të përshpejtohet edhe vetë koha e aplikimit dhe marrjes së rezultateve nga vetë aplikacioni.

Faza 3: Konsultimi

Merrni parasysh si do të konsultoheni me palët e interesuara: përshkruajeni kur dhe si do të kërkoni mendim nga personat fizikë – ose sqaroni pse kjo nuk është e përshtatshme të bëhet. Kush do të jetë tjetër i përfshirë në institucionin tuaj? A do të ketë të përfshirë edhe përpunues? A do të përfshihen konsulentë për siguri të informacionit ose konsulentë tjerë?

Para implementimit të sistemit, u konsultuan edhe personat fizikë. U dorëzua pyetësor te të gjithë personat fizikë që të vlerësohet interesimi dhe/ose shqetësimi i tyre për implementim të sistemit të tillë. Vetë sistemi përkatësisht rezultatet nga kërkesa u vërtetuan/korrigjuan nga të punësuarit në Ministrinë për zvogëlimin e gabimeve nga vetë sistemi.

Faza 4: Vlerësimi i domosdoshmërisë dhe proporcionalitetit

Përshkruani masat për harmonizim dhe proporcionalitet, konkretisht: Cila është baza ligjore për përpunim? A do të arrihet me përpunimin qëllimi i dëshiruar? A ekziston ndonjë mënyrë tjetër me të cilën mund të arrihet qëllimi i njëjtë? Si do të parandalohet që të përpunohen të dhënat personale në mënyrë të paautorizuar për qëllime tjera? Si do të arrihet cilësia e të dhënave dhe vëllimi minimal i të dhënave personale? Çilat informata do t'u jepen personave fizikë? Si garantohet realizimi i të drejtave të personave fizikë si subjekte të të dhënave personale? Cilat masa do të ndërmerren për harmonizimin e përpunuesit? Si do të mbrohen transferimet ndërkombëtare? A do të transferohen të dhënat personale në vende të treta (jashtë BE-së, shembull: ruajtja në server) Cila është arsyeja e transferimit të të dhënave personale jashtë BE-së? Cilat të dhëna personale do të transferohen jashtë BE-së? Çfarë masash do të ndërmerren gjatë transferimit të të dhënave personale? (p.sh. Përdorimi i "cloud", autoritetet e kontrollit financiar shkëmbejnë të dhëna në kontekstin e transferimit ndërkombëtar të të dhënave personale për qëllime të bashkëpunimit administrativ.

Baza ligjore e këtij përpunimi është Ligji për standardin studentor dhe Rregullorja për llojin e bursave studentore dhe mënyrën e ndarjes së bursave studentore.

Po, me përpunimin arrihet qëllimi i dëshiruar.

Nuk ekziston mënyrë tjetër për t'u arritur qëllimi i njëjtë.

Të dhënat për ato studentë që aplikojnë për marrje të bursës anonimizohen dhe ato ruhen në përputhje me Procedurën për afatet e ruajtjes, me ç'rast parandalohet qasje e paautorizuar në to. Në vetë ueb aplikacionin përpunohen të dhënat e domosdoshme, përkatësisht të dhënat e domosdoshme për realizim të qëllimit. Lidhur me cilësinë e të dhënave, vetë studenti e vërteton saktësinë e të dhënave të futura me ç'rast për përsëritjen e identitetit të përdoruesit përdoret sistem për identifikim elektronik të përdoruesit.

Informatat si dhe realizimi i të drejtave të subjekteve janë cekur në Politikën e privatësisë.

Para zgjedhjes së Përpunuesit, përgjegjës për zhvillimin e ueb aplikacionit, u konstatua (me qasje fizike në hapësirat e tij dhe kontroll të dokumentacionit të tij) se ai i aplikon dispozitat e LMDHP-së dhe me të është lidhur kontratë (klauzola kontraktuese standarde) .

Nuk ka transferim jashtë kufijve të RMV-së.

Faza 5: Identifikimi dhe vlerësimi i rreziqeve

Përshkruajeni kërcënimin	**Gjasa e kërcënimit**	**Ndikimi i kërcënimit**	**Rreziku i përgjithshëm**
paarritshmëria e sistemit	Gjasë **e vogël,** e mesme, e madhe	I ulët, i mesëm, **i lartë,** shumë i lartë	I ulët, **i mesëm** ose i lartë

Faza 6: Masat për reduktim të rrezikut

Identifikimi i masave mbrojtëse të cilat duhet të ndërmerren që të reduktohen ose eliminohen rreziqet e identifikuara me rrezik të mesëm dhe të lartë dhe shumë të lartë në fazën 5				
Rreziku	**Propozim-masa e sigurisë**	**Masa e miratuar**	**Personi përgjegjës për implementim**	**Afati i realizimit**

paaritshmëria e sistemit	*plan për rimëkëmbje nga katastrofat vendi dhe plani për vazhdimësi në punë*	***Po**/Jo*	*Shërbimi për TI*	*31.12.2023*

Faza 7: Shënimi

	Emri/pozita/data	**Shënim**
Masa të aprovuara nga:	*Emri dhe mbiemri, personi përgjegjës nga sektori, 01.01.2023*	Përfshini të gjitha aktivitetet në planin e projektit, me datë dhe përgjegjësi për realizim
Mendimi i siguruar nga OMDHP:	*Emri dhe mbiemri*	OMDHP duhet të japë mendim nëse mund të bëhet përpunimi
Përshkrimi i shkurtër i mendimit të OMDHP-së: *Oficeri konsideron se përpunimi mund të bëhet pasi të zbatohen masat e sigurisë dhe pasi të sigurohet se sistemi jep rezultate reale dhe rezultate të cilat nuk i cenojnë të drejtat dhe liritë e personave fizikë.*		
Mendimi i OMDHP-së është pranuar ose jo, nga:	*Mendimi është i pranuar nga emri dhe mbiemri.*	Nëse nuk është pranuar, sqaroni pse
Koment:/		
Përgjigjet nga konsultimet janë rishikuar nga:	*Emri dhe mbiemri, udhëheqës sektori*	Nëse vendimi juaj shmanget nga mendimi i personave fizikë, doemos duhet t'i sqaroni arsyet tuaja
Koment:/		
Këtë VNMDHP do ta ruajë:	*Emri dhe mbiemri, përgjegjës nga sektori*	OMDHP duhet ta rishikojë harmonizimin me VNMDHP

13. SHTOJCA NR.2

Lista e llojeve të operacioneve të përpunimit për të cilat kërkohet vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale

- Vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale kërkohet detyrimisht për lloje të caktuara të operacioneve të përpunimit, veçanërisht për:
- përpunim të të dhënave personale për profilizim sistematik dhe gjithëpërfshirës ose vendimmarrje automatike me qëllim për të nxjerrë konkluzione dhe të miratohen vendime që prodhojnë veprim juridik, të cilat në masë të madhe ndikojnë mbi personin fizik dhe/ose më shumë persona ose që ndihmojnë gjatë miratimit të vendimeve për qasjen e dikujt në shërbimin ose ndonjë lloj të shërbimit ose ndonjë volitshmëri (p.sh., siç janë përpunimi i informatave personale lidhur me statusin ekonomik ose financiar, shëndetin, preferencat personale, interesat, siguria, sjellja, të dhënat për lokacionin etj.)
- përpunim të kategorive të veçanta të të dhënave personale për qëllime profilizimi ose vendimmarrjeje automatike;
- përpunim të kategorive të veçanta të të dhënave personale, përkatësisht të dhënave që zbulojnë origjinën racore ose etnike, mendimin politik, bindjen fetare ose filozofike ose anëtarësimin në sindikatë, si dhe përpunimin e të dhënave gjenetike, të dhënave biometrike me qëllim identifikimin e vetëm të personave, të dhënave shëndetësore ose të dhënave për jetën seksuale ose orientimin seksual të individit;
- përpunim të gjerë të kategorive të veçanta të të dhënave personale ose të të dhënave personale lidhur me dënimet ndëshkimore dhe veprat penale (neni 14 i Ligjit për mbrojtjen e të dhënave personale) ose përgjegjësinë penale;
- përpunim të të dhënave personale të fëmijëve për qëllime profilizimi, vendimmarrjeje automatike ose për qëllime marketingu ose për ofrimin e drejtpërdrejtë të shërbimeve të dedikuara për ta;
- përpunim të të dhënave personale të mbledhura nga palët e treta (personat), të cilat merren parasysh për vendimmarrje lidhur me lidhjen, zgjidhjen, refuzimin ose vazhdimin e kontratave për ofrimin e shërbimeve për personat fizikë;
- përpunim të të dhënave personale duke përdorur mbikëqyrjen (monitorimin) sistematik të hapësirës së disponueshme publikisht në përmasa të mëdha;
- përdorim të teknologjive të reja ose zgjidhjeve teknologjike për përpunimin e të dhënave personale ose me mundësinë e përpunimit të të dhënave personale që shërbejnë për të analizuar ose parashikuar situatën ekonomike, shëndetin, dëshirat ose interesat personale, sigurinë ose sjelljen, vendndodhjen ose lëvizjen e personave fizikë;
- përpunim të të dhënave personale përmes lidhjes, krahasimit ose kryerjes së

kontrollit të ngjashmërive nga më shumë burime;

- përpunim të të dhënave personale në një mënyrë që përfshin monitorim të vendndodhjes ose sjelljes së personit fizik në rastin e përpunimit sistematik të të dhënave të komunikimit (meta të dhëna) të krijuara- të gjeneruara me përdorimin e telefonit, internetit ose pajisjeve (kanaleve) të tjera të komunikimit, siç janë GSM, GPS, Wi-Fi, për monitorim dhe përpunim të të dhënave për vendndodhje;
- përpunim të të dhënave personale nëpërmjet përdorimit të pajisjeve dhe teknologjive, te të cilat, nëse ndodh incident, mund ta rrezikojë shëndetin e një ose më shumë personave (subjekte të të dhënave personale); dhe përpunim të kategorive të veçanta të të dhënave personale të punonjësve që përdoren për identifikim unik të punonjësve nga punëdhënësi dhe në raste të tjera të përpunimit të të dhënave për personat – punonjësit nga punëdhënësi nëpërmjet përdorimit të aplikacionit ose sistemit për monitorimin e punës, lëvizjes dhe komunikimit të tyre etj. (p.sh. përpunimi i të dhënave personale për kryerje të monitorimit të detyrimeve të punës, lëvizjes, komunikimit, etj.).

14. SHTOJCA NR.3

LISTA E AKTIVITETEVE PËR TË CILAT NUK KËRKOHET VNMDHP

Vlerësimi i ndikimit mbi mbrojtjen e të dhënave personale nuk kërkohet për lloje të caktuara të operacioneve të përpunimit, veçanërisht kur:

- aktivitetet e përpunimit nuk rezultojnë me rrezik të lartë për të drejtat dhe liritë e personave fizikë;
- proceset (aktivitetet) janë përcaktuar paraprakisht se nuk janë ekspozuar ndaj rrezikut gjatë vlerësimit të ndikimit ndaj mbrojtjes së të dhënave personale;
- përpunimi është miratuar tashmë nga Agjencia për Mbrojtjen e të Dhënave Personale;
- për përpunimin ekziston tashmë një bazë ligjore ekzistuese e qartë dhe specifike në sistemin juridik të Republikës së Maqedonisë së Veriut dhe kur vlerësimi i ndikimit në mbrojtjen e të dhënave personale është kryer tashmë si pjesë e vendosjes së asaj baze ligjore sipas nenit 10 paragrafi (3) të Ligjit për mbrojtjen e të dhënave personale;
- kryhet si pjesë e vlerësimit të ndikimit që rrjedh nga baza e interesit publik dhe kur vlerësimi i ndikimit në mbrojtjen e të dhënave personale ka qenë element i atij

vlerësimi sipas nenit 10 paragrafi (3) të Ligjit për mbrojtjen e të dhënave personale.

- Këtë Listë e përcakton Agjencia për Mbrojtjen e të Dhënave Personale. Oficeri për mbrojtjen e të dhënave personale për obligim t'i monitorojë ndryshimet dhe ato t'i implementojë në sistemin e institucionit.

15. SHTOJCA NR.4

ANEKSI I I AKTIT
TEKNIKAT DHE QASJET E INTELIGJENCËS ARTIFICIALE

Neni 3 pika 1 e Aktit

(a) Qasje për mësim makinerik, përfshirë mësimin nën mbikëqyrje, mësimin pa mbikëqyrje si dhe përforcimin e mësimit, duke përdorur spektër të gjerë të metodave përfshirë edhe mësimin e thellë;

(b) Qasjet e bazuara në logjikë dhe njohuri, përfshirë edhe prezantimin e njohurisë, programim induktiv (logjik), baza të njohurive, motorë inferencialë dhe deduktivë (eng. Inferential and deductive engines), gjykim (simbolik) dhe sisteme ekspertësh;

(c) Qasje statistikore, vlerësimi i Bajesit (eng. Bayesian estimation), metodat për kërkim dhe optimizim.

16. SHTOJCA NR. 5

ANEKSI III I AKTIT
SISTEMET E IA-SË ME RREZIK TË LARTË TË CEKURA NË NENIN 6(2)

Sistemet e inteligjencës artificiale me rrezik të lartë në përputhje me nenin 6(2) janë sisteme të inteligjencës artificiale të cekura në cilëndo prej sferave në vijim:

1. Identifikimi biometrik dhe kategorizimi i personave fizikë:

(a) Sistemet për inteligjencë artificiale të dedikuara për t'u përdorur për identifikim biometrik në distancë të personave fizikë "në kohë reale dhe në kohë joreale";

2. Menaxhimi dhe funksionimi i infrastrukturës kritike:

(a) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur si komponentë të sigurisë në menaxhimin dhe funksionimin e komunikacionit rrugor dhe furnizimin me ujë, gaz, ngrohje qendrore dhe energji elektrike.

3. Arsimi dhe aftësimi profesional:

(a) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur për qëllimet për caktim të qasjes ose shpërndarjes së personave fizikë në institucione arsimore dhe profesionale;

(b) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur për qëllimet e vlerësimit të studentëve në institucionet arsimore dhe profesionale dhe për vlerësim të nxënësve të testeve të cilat zakonisht janë të nevojshme për pranim në institucionet arsimore.

4. Punësimi, menaxhimi me të punësuarit dhe qasja në vetëpunësim:

(a) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur për rekrutim ose zgjedhje të personave fizikë, veçanërisht për shpallje të vendeve të lira të punës, skrining ose filtrim të aplikacioneve për punësim, vlerësim të kandidatëve gjatë intervistës ose testeve;

(b) Sisteme e inteligjencës artificiale të dedikuara për t'u përdorur për vendimmarrje për avancim dhe ndërprerje të marrëdhënieve kontraktuese lidhur me punën, për shpërndarje të detyrave dhe për monitorim dhe vlerësim të performancave dhe sjelljes së punonjësve ose personave të angazhuar.

5. Qasje në dhe gëzim të shërbimeve dhe përfitimeve private dhe publike:

(a) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur nga ose në emër të organeve publike për ta vlerësuar përshtatshmërinë e personave fizikë për përfitime dhe shërbime për ndihmë publike, si dhe për ndarje, zvogëlim, revokim ose kthim të përfitimeve dhe shërbimeve të tilla;

(b) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur për vlerësim të aftësisë kreditore të personave fizikë ose për të përcaktuar rejtingun e tyre të kredisë, me përjashtim të sistemeve të inteligjencës artificiale të vendosura në shërbim nga provjderët e vegjël për përdorimin e tyre;

(c) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur për dërgim ose për përcaktim të prioritetit në dërgimin e shërbimeve në raste urgjente, përfshirë edhe zjarrfikësit dhe ndihmën mjekësore.

6. Zbatimi i ligjit:

(a) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur nga organet e zbatimit të ligjit për përpunim të vlerësimeve individuale të rrezikut të personave fizikë, me qëllim të vlerësimit të rrezikut që personi fizik të kryejë vepër në kundërshtim me ligjin ose rrezikun e viktimave të mundshme të veprave penale;

(b) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur nga organet e zbatimit të ligjit si poligrafi dhe mjete të ngjashme ose për të zbuluar gjendjen emocionale të një personi fizik;

(c) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur nga autoritetet e zbatimit të ligjit për të zbuluar falsifikime të thella siç është cekur në nenin 52(3) të Aktit;

(ç) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur nga organet e zbatimit të ligjit për të vlerësuar besueshmërinë e provave gjatë hetimit ose gjatë ndjekjes së autorëve të veprave penale;

(d) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur nga organet e zbatimit të ligjit për të parashikuar ndodhjen ose ndodhjen e sërishme të veprës së vërtetë ose potenciale penale të bazuar në profilizimin e personave fizikë siç është cekur në nenin 3(4) të Direktivës (BE) 2016/680 ose vlerësim të tipareve dhe karakteristikave të personalitetit ose sjelljes së kaluar kriminale të të personave fizikë ose grupeve të personave fizikë;

(dh) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur nga organet e zbatimit të ligjit për të profilizuar personat fizikë siç është cekur në nenin 3(4) të Direktivës (BE) 2016/680 gjatë zbulimit, hetimit ose ndjekjes së autorëve të veprave penale;

(e) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur për analitikë të krimit kundër personave fizikë, duke lejuar organet e zbatimit të ligjit të kërkojnë grupe të mëdha, të ndërlikuara të lidhura dhe të palidhura të të dhënave të disponueshme nga burime të ndryshme të dhënash ose në formate të ndryshme të dhënash me qëllim të identifikimit të skemave të panjohura ose të zbulimit të marrëdhënieve të fshehura në të dhënat.

7. Menaxhimi me migrimin, azilin dhe kontrollin kufitar:

(a)Sistemet e inteligjencës artificiale të dedikuara për organet kompetente shtetërore si poligrafi dhe mjete të ngjashme ose për të zbuluar gjendjen emocionale të një personi fizik;

(b) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur nga organet kompetente shtetërore për të vlerësuar rrezikun, përfshirë rrezikun e sigurisë, rrezikun e imigrimit të parregullt ose rrezikun shëndetësor të një personi fizik që synon të hyjë ose ka hyrë në territorin e një shteti anëtar i BE-së;

(c) Sistemet e inteligjencës artificiale të dedikuara për t'u përdorur nga organet kompetente shtetërore për të kontrolluar autenticitetin e dokumenteve të udhëtimit dhe dokumentacionit shoqërues të personave fizikë dhe për zbulimin e dokumenteve joautentike duke kontrolluar karakteristikat e tyre të sigurisë;

(ç) Sistemet e inteligjencës artificiale të dedikuara për t'u ndihmuar organeve shtetërore kompetente për shqyrtimin e kërkesave për azil, vizë dhe leje qëndrimi dhe ankesave të lidhura lidhur me përshtatshmërinë e personave fizikë që aplikojnë për ndonjë status.

8. Menaxhimi i drejtësisë dhe proceseve demokratike:

(a) Sistemet e inteligjencës artificiale të dedikuara për t'i ndihmuar organit gjyqësor në hetimin dhe interpretimin e fakteve dhe ligjit dhe gjatë aplikimit të të drejtës së zgjedhjes konkrete të fakteve.

17. SHTOJCA NR. 6

ANEKSI VI NGA AKTI
PROCEDURA E VLERËSIMIT TË PËRSHTATSHMËRISË TË BAZUAR NË KONTROLLIN E BRENDSHËM

1. Procedura e vlerësimit të përshtatshmërisë të bazuar në kontrollin e brendshëm është bazuar në pikat 2, 3 dhe 4;

2. Provajderi vërteton se sistemi i implementuar për menaxhim me cilësinë është në përputhje me kërkesat e Aktit;

3. Provajderi i kontrollon informatat e përfshira në dokumentacionin teknik që të vlerësohet harmonizimi i sistemit të IA-së me kërkesat e domosdoshme relevante të cekura në Aktin;

4. Provajderi gjithashtu vërteton se procesi i dizajnimit dhe zhvillimit të sistemit të IA-së dhe monitorimi i tij pas lëshimit në treg të cekur në Aktin është në përputhje me dokumentacionin teknik;

18. SHTOJCA NR.7

ANEKSI VII I AKTIT
VLERËSIMI I PËRSHTATSHMËRISË I BAZUAR NË VLERËSIMIN E SISTEMIT PËR MENAXHIM ME CILËSINË DHE VLERËSIMI I DOKUMENTACIONIT TEKNIK

1. Hyrje

Përputhshmëria në bazë të vlerësimit të sistemit për menaxhim me cilësinë dhe vlerësimi i dokumentacionit teknik është procedurë për vlerësim të përshtatshmërisë të bazuar në pikat 2 deri 5.

2. Kontrolli

Sistemi i miratuar për menaxhim me cilësinë për dizajn, zhvillim dhe testim të sistemeve për inteligjencë artificiale në përputhje me nenin 17 do të kontrollohet në përputhje me pikën 3 dhe do të jetë objekt i mbikëqyrjes siç është cekur në pikën 5. Dokumentacioni teknik i sistemit të IA-së do të kontrollohet në përputhje me pikën 4.

3. Sistemi për menaxhim me cilësinë

3.1. Aplikacioni i provajderit do të përfshijë**:**

(a) emrin dhe adresën e provajderit dhe, nëse aplikimi është bërë nga përfaqësues i autorizuar, gjithashtu edhe emrin dhe adresën e tyre;

(b) listën e sistemeve të inteligjencës artificiale të përfshira me sistemin e njëjtë për menaxhim me cilësinë;

(c) dokumentacionin teknik për çdo sistem të inteligjencës artificiale të mbuluar me sistemin e njëjtë të menaxhimit me cilësinë;

(ç) dokumentacionin në lidhje me sistemin për menaxhim me cilësinë e cila do t'i mbulojë të gjitha aspektet e cekura në nenin 17;

(d) përshkrim të procedurave që janë vendosura për të siguruar që sistemi i menaxhimit me cilësinë mbetet adekuat dhe efektiv;

(dh) deklaratë me shkrim se aplikimi i njëjtë nuk është parashtruar te asnjë organi tjetër i autorizuar.

3.2. Sistemi i menaxhimit të cilësisë do të vlerësohet nga organi i autorizuar i cili do të përcaktojë nëse i plotëson kërkesat e përcaktuara në nenin 17. Për vendimin do të njoftohet provajderi ose përfaqësuesi i tij i autorizuar. Njoftimi përmban konkluzionet e vlerësimit të sistemit për menaxhim me cilësinë dhe vendimin e arsyetuar në bazë të vlerësimit.

3.3. Sistemi për menaxhim me cilësinë siç është miratuar do të vazhdojë të implementohet dhe të mirëmbahet nga provajderi që të mbetet adekuat dhe efikas.

3.4. Çdo ndryshim i planifikuar i sistemit tashmë të miratuar për menaxhim me cilësisë ose lista e sistemeve të inteligjencës artificiale të përfshira nga ai do t'i dorëzohen për vëmendje organit të autorizuar nga provajderi.

Ndryshimet e propozuara do të shqyrtohen nga organi i autorizuar i cili do të vendosë nëse sistemi i modifikuar për menaxhim me cilësinë vazhdon t'i përmbushë kërkesat e përcaktuara në pikën 3.2 ose nëse nevojitet rivlerësim.

Organi i autorizuar do të njoftojë provajderin për vendimin e tij. Njoftimi do t'i përmbajë konkluzionet e vlerësimit të ndryshimeve dhe shkaqet për vendimin e miratuar nga vlerësimi.

4. Kontrolli i dokumentacionit teknik

4.1. Bashkëngjitur me aplikimin nga pika 3, aplikimi me organin e autorizuar sipas zgjedhjes së tyre do të parashtrohet nga provajderi për vlerësim të dokumentacionit teknik që i referohet sistemit për inteligjencë artificiale për të cilin provajderi ka për qëllim ta plasojë në treg ose ta lëshojë në përdorim dhe i cili është i mbuluar me sistemin për menaxhim me cilësi të cekur në pikën 3.

4.2. Aplikacioni do të përfshijë:

(a) emrin dhe adresën e provajderit;

(b) deklaratën me shkrim se aplikimi i njëjtë nuk iu është parashtruar asnjë organi tjetër të autorizuar;

(c) dokumentacionin teknik të Aktit.

4.3. Organi i autorizuar e shqyrton dokumentacionin teknik. Për këtë qëllim, organit të autorizuar do t'i jepet qasje e plotë në trajnimin dhe testimin e përmbledhjeve të të dhënave të cilat i përdor provajderi, përfshirë interfejset për programim të aplikacioneve (API) ose mjetet dhe veglat e tjera përkatëse që mundësojnë qasje në distancë.

4.4. Gjatë shqyrtimit të dokumentacionit teknik, organi i autorizuar mund të kërkojë që provajderi të sigurojë prova shtesë ose të kryejë teste shtesë për të mundësuar vlerësim të duhur të harmonizimit të sistemit të inteligjencës artificiale me kërkesat e përcaktuara në Aktin. Gjithmonë kur organi i autorizuar nuk është i kënaqur me testet që i ka kryer provajderi, organi i autorizuar do të kryejë drejtpërdrejt teste përkatëse.

4.5. Atje ku është e nevojshme të vlerësohet përputhshmëria e sistemit të inteligjencës artificiale me rrezik të lartë me kërkesat e përcaktuara në Aktin dhe me kërkesë të arsyetuar, aorgani mbikëqyrës do të ketë gjithashtu qasje në

kodin burimor të sistemit të inteligjencës artificiale.

4.6. Për vendimin njoftohet provajderi ose përfaqësuesi i tij i autorizuar. Njoftimi do të përmbajë konkluzionet e vlerësimit të dokumentacionit teknik dhe vendimin e arsyetuar për vlerësimin.

Kur sistemi i inteligjencës artificiale është në përputhje me kërkesat e përcaktuara në Aktin, organi i autorizuar lëshon certifikatë të BE-së për vlerësimin e dokumentacionit teknik. Në certifikatë ceket emri dhe adresa e provajderit, konkluzionet nga shqyrtimi, kushtet (nëse ka) për vlefshmërinë e saj dhe të dhënat e domosdoshme për identifikimin e sistemit të inteligjencës artificiale.

Certifikata dhe anekset e tij i përmbajnë të gjitha informatat relevante që të mundësohet vlerësimi i përputhshmërisë së sistemit për inteligjencë artificiale dhe të mundësohet kontroll i sistemit për inteligjencë artificiale përderisa është në përdorim, atje ku është e aplikueshme.

Kur sistemi për inteligjencë artificiale nuk është në përputhje me kërkesat e cekura në Aktin, organi i autorizuar do të refuzojë të lëshojë certifikatë të BE-së për vlerësim të dokumentacionit teknik dhe do ta njoftojë në mënyrë adekuate kërkuesin, duke dhënë arsye për refuzimin e tij.

Atje ku sistemi për inteligjencë artificiale nuk e përmbush kushtin lidhur me të dhënat që përdoren për trajnim të sistemit, do të nevojitet përsëri trajnim të sistemit të inteligjencës artificiale para se aplikojë për vlerësim të ri të përputhshmërisë. Në këtë rast vendimi i arsyetuar nga vlerësimi i organit mbikëqyrës i cili refuzon ta lëshojë certifikatën e BE-së për vlerësim të dokumentacionit teknik do të përmbajë mendime konkrete për cilësinë e të dhënave të cilat do të përoden për trajnim të sistemit për inteligjencë artificiale, veçanërisht për shkaqet e mosharmonizimit.

4.7. Çdo ndryshim i sistemit për inteligjencë artificiale që mund të ndikojë në harmonizimin e sistemit për inteligjencë artificiale kërkesën ose dedikimin e tij e miraton organi i autorizuar i cili e ka lëshuar certifikatën e BE-së për vlerësim të dokumentacionit teknik. Provajderi do ta njoftojë organin e tillë të autorizuar për qëllimin e tij për të sjellë ndonjë prej ndryshimeve të lartpërmendura ose në mënyrë tjetër bëhet i vetëdijshëm për paraqitjen e ndryshimeve të tilla. Ndryshimet e parapara i vlerëson organi i autorizuar i cili do të vendosë nëse ato ndryshime kërkojnë vlerësim të ri të përputhshmërisë me Aktin, ose nëse ato mund të zgjidhen me ndihmën e plotësimit të certifikatës së BE-së për vlerësim të dokumentacionit teknik. Në rastin e dytë, organi i autorizuar do t'i vlerësojë ndryshimet, do ta njoftojë provajderin për vendimin e tij dhe ku ndryshimet janë miratuar, provajderit do t'i lëshojë certifikatë të BE-së për vlerësim të dokumentacionit teknik.

5. Mbikëqyrja e sistemit të miratuar për menaxhim me cilësinë.

5.1. Qëllimi i mbikëqyrjes të cilën e kryen organi i autorizuar të cekur në pikën 3 është të bindet se provajderi i përmbush në mënyrë adekuate kushtet dhe dispozitat nga sistemi i miratuar për menaxhim me cilësinë.

5.2. Për qëllimet e ndryshimit, provajderi i lejon organit të autorizuar qasje në hapësirat në të cilat realizohet dizajni, zhvillimi, testimi i sistemeve për inteligjencë artificiale. Provajderi në mënyrë plotësuese do t'i ndajë me organin e autorizuar të gjitha informatat e nevojshme.

5.3. Trupi i autorizuar kryen revizione periodike që të bindet se provajderi e mirëmban dhe e aplikon sistemin për menaxhim me cilësinë dhe do t'i dorëzojë provajderit raport të revizorit. Në kontekst të atyre revizioneve, organi i autorizuar mund të kryejë teste plotësuese të sistemeve për inteligjencë artificiale për të cilat është lëshuar certifikatë e BE-së për vlerësim të dokumentacionit teknik.