

FOL

Doracak me 10 skenarë të reagimit rreth shkeljes së të dhënave personale



**Doracak me 10
skenarë të reagimit
rreth shkeljes së të
dhënave personale
në institucionet
publike dhe private**

Ky dokument është realizuar si pjesë e projektit "Human Rightivism", në kuadër të nismës "Gardianët e të dhënave: Forcimi i Politikave të Privatësisë dhe Ndërgjegjësimit në Institucionet Publike" që udhëhiqet nga Lëvizja FOL. Projekti implementohet nga Fondi për Zhvillim Komunitar (CDF) me mbështetjen e Ambasadës së Suedisë në Prishtinë.



Ky dokument u zhvillua në bashkëpunim me Agjencinë për Informim dhe Privatësi.

VITI I BOTIMIT:
2024

PUBLIKUAR NGA:
Lëvizja FOL

WEBSITE:
www.levizjafol.org

ADRESA:
Andrea Gropa nr.35, Prishtinë 10000, Republika e Kosovës

E drejta e autorit © 2024. Lëvizja FOL. Të gjitha të drejtat e rezervuara. Asnjë pjesë e këtij publikimi nuk mund të riprodhohet, ruhet në një sistem rikthimi, ose të transmetohet, në çfarëdo forme ose me çfarëdo mjeti, elektronik, mekanik, fotokopjues, incizues ose ndryshe, pa pëlqimin paraprak me shkrim të publikuesit.

Përmbajtja

SKENARI 1:	Mungesa e konfidencialitetit në ndarjen e diagnozave shëndetësore	06
SKENARI 2:	Fotografimi dhe filmimi i pacientëve	12
SKENARI 3:	Publikimi i të dhënave të pacientëve për trajtim jashtë vendit	18
SKENARI 4:	Kërkesat për të dhëna gjenetike nga kompanitë e sigurimeve shëndetësore	24
SKENARI 5:	Vendosja e kamerave të mbikëqyrjes nga institucionet publike dhe private	30
SKENARI 6:	Përpunimi i të dhënave nga institucionet publike dhe private të telekomunikacionit	36
SKENARI 7:	Përdorimi i kamerave dhe përpunimi i të dhënave në institucionet parashkollore	42
SKENARI 8:	Përdorimi i kamerave dhe përpunimi i të dhënave në institucionet shkollore	48
SKENARI 9:	Marketingu i drejtpërdrejtë - SMS dhe thirrje telefonike të pandërprera	55
SKENARI 10:	Transferimi i të dhënave personale nga bankat	62

Hyrje

Privatësia dhe mbrojtja e të dhënave personale janë të drejta themelore të njeriut, të cilat luajnë një rol të rëndësishëm në jetën e përditshme, veçanërisht në një shoqëri gjithnjë e më të ndërlidhur dhe të dixhitalizuar. Shkelja e privatësisë dhe përpunimi i paautorizuar i të dhënave personale janë shqetësime të mëdha që prekin të gjithë qytetarët, si në sektorin publik ashtu edhe në atë privat.

Ky dokument, "Skenarët për Shkeljen dhe Mbrojtjen e të Dhënave Personale," është hartuar nga Lëvizja FOL në kuadër të Projektit "Gardianët e të Dhënave: Forcimi i Politikave të Privatësisë dhe Ndërgjegjësimi në Institucionet Publike", përmes Human Rightivism që mbështetet nga Ambasada e Suedisë në Kosovë përmes Community Development Fund – CDF. Ky dokument ka për qëllim që të ofroj një pasqyrë të qartë dhe gjithëpërfshirëse mbi situatat e përditshme ku privatësia dhe të dhënat personale mund të shkelën, si dhe për të ndihmuar qytetarët të kuptojnë të drejtat e tyre ligjore dhe hapat që mund të ndërmarrin për t'i mbrojtur ato. Ligji i cituar në këtë dokument është Ligji nr.06/L-082 për mbrojtjen e të dhënave personale.

Çdo skenar pasqyron sfidat reale me të cilat mund të përballen qytetarët e Kosovës në lidhje me privatësinë dhe përpunimin e të dhënave personale, duke përfshirë obligimet ligjore të institucioneve përkatëse dhe veprimet që mund të ndërmarrin qytetarët për të siguruar mbrojtjen e të drejtave të tyre.

Ky dokument u zhvillua duke përfshirë kontributin nga takimet e Fokus Grupit dhe sugjerimet e profesionistëve të fushës, me qëllim që të jetë një udhëzues praktik dhe edukativ për të gjithë ata që kërkojnë të kuptojnë më mirë të drejtat e tyre në lidhje me mbrojtjen e të dhënave personale.

Besojmë që ky material të shërbejë si një burim i vlefshëm për ngritjen e vetëdijes dhe përmirësimin e praktikave të mbrojtjes së privatësisë në Kosovë.

SKENARI 1:

**Mungesa e
konfidencialitetit
në ndarjen e
diagnozave
shëndetësore**

Ligji kërkon që çdo
informacion rreth
shëndetit tënd të ruhet
me konfidencialitet dhe që
askush të mos ketë qasje
pa lejen tënde!



SKENARI 1:

Mungesa e konfidencialitetit në ndarjen e diagnozave shëndetësore



Arjeta, një grua 48-vjeçare, shkon në një klinikë në Prishtinë për një kontroll rutinë. Ndërsa pret në korridor, një infermiere fillon t'i bëjë pyetje personale në lidhje me historikun e saj mjekësor, duke përfshirë operacionet dhe sëmundjet e kaluara, në prani të pacientëve dhe stafit tjetër që nuk është drejtëpërdrejtë duke i shërbyer/ndihmuar asaj.

Këto pyetje të hapura e bëjnë Arjetën të ndihet e ekspozuar dhe në siklet, pasi detajet e ndjeshme të shëndetit të saj diskutohen publikisht, pa pasur fare respekt për privatësinë e saj.

Po ashtu, më vonë, kur dolën rezultatet, dokumenti me diagnozën e saj u la në një tavolinë të hapur ku mund të qasej nga gjithkush që është afër.

Ky skenar ngritë pyetje mbi shkeljen e privatësisë dhe respektit për të dhënat personale brenda ambienteve të kujdesit shëndetësor në Kosovë, ku informacionet konfidenciale shpesh ndahen pa diskrecion të duhur.

Cilat ish in obligimet e institucionit përkatës në rastin konkret?

Baza ligjore: Ligji, neni 3, paragrafi 1.25, neni 5 paragrafi 1.1, neni 8 paragrafi 2.1.

- **Institucioni duhet të kishte infraskturën e duhur që lejon mbrojtjen e të dhënave:**

Institucioni mund të caktojë vetë metodat që janë të aplikueshme për të siguruar që të dhënat personale mbrohen (dhomat e veçanta për marrjen e të dhënave, formularët specifik, forma të tjera që përcaktohen nga vetë kontrolluesi, etj), për aq sa këto metoda sigurojnë mbrojtjen e të dhënave dhe pajtueshmërinë me ligjin.

- **Regjistri i aktiviteteve të përpunimit:** Institucioni duhet të mbajë një regjistër të aktiviteteve të përpunimit me të dhënat si përcaktohet në ligj.

Baza ligjore: Ligji, neni 29.

- **Hartimi i akteve të brendshme për përpunim:** Institucioni shëndetësor në fjalë duhet të ketë aktet e brendshme në të cilat duhet të rregullohen aspektet që kanë të bëjnë me procedurat dhe masat e vendosura për sigurinë e të dhënave personale.

Baza ligjore: Ligji, neni 40.

- Krijimin e zyrës për mbrojtjen e të dhënave dhe trajnimi i specializuar/certifikuar i zyrtarëve në pajtim me nenet 37-40 dhe 43 të Ligjit.

Çka mund të bënte Arjeta në skenarin e përshkruar?

Bazuar në Ligjin për Mbrojtjen e të Dhënave Personale, Arjeta mund të ndër-marrë veprimet e mëposhtme:

Kërkesë për qasje në të dhënat personale: Arjeta ka të drejtë të kërkojë qasje në të dhënat e saj personale për të ditur se kush ka pasur akses në to dhe nëse ka pasur përpunim të paautorizuar, në bazë të nenit 14.

Kërkesë për fshirjen e të dhënave të përpunuara pa pëlqimin e saj: Nëse dokumenti me diagnozën e saj është lënë i qasshëm për të tjerët pa lejen e saj, ajo ka të drejtë të kërkojë fshirjen e të dhënave, bazuar në nenin 16.

Ankesë tek Agjencia për Informim dhe Privatësi: Arjeta mund të paraqesë një ankesë tek Agjencia për të kërkuar hetimin e shkeljes së konfidencialitetit dhe marrjen e masave për mbrojtjen e të dhënave të saj personale, në përputhje me nenin 52.

Kërkesë për korigjim ose kufizim të përpunimit: Nëse Arjeta beson se të dhënat e saj janë përpunuar në mënyrë të paautorizuar, ajo mund të kërkojë korigjimin ose kufizimin e përpunimit të të dhënave, sipas nenit 17.

Padi për kompensim të dëmeve: Arjeta mund të bëjë padi për kompensim të dëmeve materiale dhe jomateriale, për shkeljet e të drejtave të saj, sipas nenit 56 të Ligjit.

SKENARI 2:

Fotografimi dhe filmimi i pacientëve

Privatësia e pacientëve
nuk është option – është e
drejtë themelore!



SKENARI 2:

Fotografimi dhe filmimi i pacientëve



Fatoni, një 33-vjeçar, po merr trajtim në një spital në Pejë pas një aksidenti me veturë. Gjatë qëndrimit të tij në korridor, në pritje të trajtimit, një stacion televiziv lokal vjen për të mbuluar një histori nga dhoma e urgjencës. Gazetarët e filmojnë Fatonin pa pëlqimin e tij, duke kapur dëmtimet dhe gjendjen e tij të brishtë. Pamjet transmetohen më pas në lajmet e mbrëmjes, duke treguar gjendjen e Fatonit për të gjithë ata që ndoqën lajmet. Të nesërmen, nga telefonatat e shumta Fatoni kuptoj se të gjithë familjarët dhe miqtë ishin tronditur me pamjet të cilat i kishin parë, duke e bërë atë të përjetoj një shqetësim të madh emocional për shkak të ekspozimit të gjendjes së tij pa lejen e tij. Kjo shkelje e privatësisë shkakton shqetësim për Fatonin dhe familjen e tij, duke theksuar rëndësinë e standardeve ligjore dhe etike kur bëhet fjalë për raportimin mediatik në mjediset e kujdesit shëndetësor në Kosovë.

Cilat ish in obligimet konkrete të gazetarëve në rastin konkret?

- **Ndjekja e hapave për lejen e incizimit brenda klinikave:** Ekziston politika e caktuar për të kërkuar leje për incizime brenda klinikave. Gazetarët duhet të garantojnë që këto procedura janë ndjekur.
- **Kodi i etikës:** Gazetarët dhe trupat vetë-rregulluese të gazetarisë duhet të sigurojnë respektimin ligjit për mbrojtjen e të dhënave personale dhe të kodit të etikës së gazetarisë

Rekomandohet: që institucionet përkatëse nga kjo fushë të vendosin dhe promovojnë kriteret orientuese për caktimin e interesit të publikut si dhe të udhëzojnë gazetarët mbi nevojën e marrjes së pëlqimit për rastet kur të dhënat personale kaq të ndjeshme janë në pyetje.

Çka mund të bënte Fatoni në skenarin e përshkruar?

Bazuar në Ligjin për Mbrojtjen e të Dhënave Personale, Fatoni mund të ndër-marrë veprimet e mëposhtme:

Kërkesë për fshirje të të dhënave: Fatoni ka të drejtë të kërkojë fshirjen e pamjeve të tij nga media që janë transmetuar pa pëlqimin e tij, duke u bazuar në nenin 16.

Kërkesë për kufizimin e përpunimit: Ai mund të kërkojë kufizimin e përpunimit të të dhënave të tij personale deri sa të sigurohet që këto janë përpunuar me bazë ligjore, në bazë të nenit 17.

Ankesë tek Agjencia për Informim dhe Privatësi: Fatoni mund të paraqesë një ankesë tek Agjencia për të kërkuar hetimin e shkeljes së privatësisë së tij dhe për të marrë masa që sigurojnë që të dhënat e tij të mbrohen, në përputhje me nenin 52.

Kërkesë për kompensim: Fatoni ka të drejtë të bëjë padi për kompensim të dëmeve materiale dhe jomateriale, për shkak të shkeljes së të drejtave të tij dhe ndikimit që transmetimi i pamjeve ka pasur në punën dhe jetën e tij personale, në përputhje me nenin 56.

SKENARI 3:

**Publikimi i të
dhënave të
pacientëve për
trajtim jashtë
vendit**

Respektimi i dinjitetit dhe
privatësisë së pacientëve
është detyrim, jo zgjedhje!



SKENARI 3:

Publikimi i të dhënave të pacientëve për trajtim jashtë vendit



Donjeta, një vajzë 6-vjeçare nga Gjilani, ka një problem serioz me veshkat dhe ka nevojë për trajtim urgjent jashtë vendit. Për të mbledhur fonde, familja e Donjetës ndjen se nuk kishte zgjidhje tjetër përveçse të kërkonte ndihmë në një medium dhe në një organizatë bamirësie. Për të dëshmuar sëmundjen e vajzës tek këto palë, familja e Donjetës, i ndanë të dhënat mbi diagnozën e saj me mediumin dhe organizatën në fjalë. Pas kësaj këto palë bënë një postim publik me thirrjen për të financuar trajtimin e Donjetës, i cili postim përfshinte edhe detaje mbi diagnozën mjeksore dhe llojin e sëmundjes nga e cila vuante Donjeta. Postimi arriti qindra mijëra njerëz, disa prej të cilëve u tallën me familjen e saj edhe për shkak të varfërisë dhe përkatësisë sociale të cilës i përkisnin.

Bazuar në Ligjin për Mbrojtjen e të Dhënave Personale, familja e Donjetës mund të ndër marrë veprimet e mëposhtme:

- **Kërkesë për fshirje të të dhënave personale:** Familja e Donjetës mund të kërkojë fshirjen e postimeve dhe çdo të dhënë të ndjeshme mbi gjendjen shëndetësore të vajzës së tyre, që është publikuar pa mbrojtje adekuate, në bazë të nenit 16.
- **Ankesë tek Agjencia për Informim dhe Privatësi:** Nëse të dhënat janë ndarë pa pëlqimin e tyre, familja mund të paraqesë një ankesë për hetim dhe për të marrë masa ndaj entiteteve që kanë publikuar këto të dhëna pa mbrojtje, sipas nenit 52.
- **Kërkesë për kufizimin e përpunimit:** Ata mund të kërkojnë që mediumi dhe organizatat bamirëse të kufizojnë përpunimin e mëtejshëm të të dhënave të vajzës së tyre, në përputhje me nenin 17.
- **Padi për kompensim të dëmeve:** Familja mund të bëjë padi për kompensim të dëmeve materiale dhe jomateriale, për shkak të shkeljes së të drejtave të Donjetës dhe dëmit që mund t'i jetë shkaktuar familjes si rezultat i ekspozimit të detajeve të ndjeshme të vajzës së tyre, në përputhje me nenin 56.

Cilat kanë qenë obligimet e institucioneve të përfshira:

- Institucioni/organizata është përgjegjëse për vlerësimin dhe mbrojtjen e të dhënave edhe nëse prindërit e Donjetës nuk kanë qenë të qartë sa i përket llojit të pajtimit për procesim.
- Duhet kryer një hulumtim i përgjithshëm mbi gjendjen aktuale të politikave të privatësisë për mediat dhe organizatat.

SKENARI 4:

**Kërkesat për të
dhëna gjenetike
nga kompanitë
e sigurimeve
shëndetësore**

Shpërndarja e të dhënave
të ndjeshme kërkon dhënien
e pëlqimit të qartë dhe
arsyetimit të fortë!



SKENARI 4:

Publikimi i të dhënave të pacientëve për trajtim jashtë vendit



Arbeni, një 52-vjeçar i siguruar me një kompani lokale sigurimesh shëndetësore, dorëzon një kërkesë për rimbursim të trajtimit të kancerit. Kompania e sigurimeve kërkon testet e tij mjekësore të detajuara, përfshirë të dhënat gjenetike, të cilat janë kryer për të vlerësuar rrezikun e tij për sëmundje të trashëguara. Edhe pse Arbeni ndihet në siklet për ndarjen e këtij informacioni të ndjeshëm, ai ka frikë se kërkesa e tij do të refuzohet nëse nuk i përmbush kërkesat. Ky skenar ilustron praktikat detyruese që mund të ndodhin në proceset e sigurimeve shëndetësore në Kosovë, ku të dhënat personale shpesh kërkohen pa pëlqim të mjaftueshëm ose justifikim.

Cilat janë veprimet e rekomanduara për Arbenin?

- **Refuzimi i përpunimit të të dhënave gjenetike pa pëlqim të qartë:** Arbeni ka të drejtën të **refuzojë përpunimin e të dhënave të tij gjenetike** nëse ato nuk janë të domosdoshme për përmbushjen e kërkesës për rimbursim, bazuar në **Nenin 8** të ligjit, i cili përcakton që të dhënat gjenetike dhe të dhënat e ndjeshme duhet të përpunohen vetëm me pëlqimin e qartë dhe në raste shumë specifike. Kompania e sigurimeve duhet të ketë një **arsyetim të qartë ligjor** për të kërkuar të dhënat e tilla, dhe Arbeni ka të drejtë të kërkojë sqarime mbi **arsyetimin dhe qëllimin** e marrjes së këtyre të dhënave.
- **Kërkesa për transparencë dhe qasje në informacion:** Arbeni mund të **kërkojë qasje në të dhënat personale** të përpunuara nga kompania e sigurimeve, duke u bazuar në **Nenin 14**.

Ai ka të drejtë të dijë:

- Pse po kërkohen të dhënat e tij gjenetike;
- Si do të përpunohen ato të dhëna dhe për sa kohë do të ruhen;
- Kush do të ketë qasje në të dhënat e tij.

- **Kërkesa për kufizim të përpunimit:** Arbeni ka të drejtën, sipas **Nenit 17**, të **kërkojë kufizimin e përpunimit** të të dhënave të tij personale deri sa të sigurohet që kompania e sigurimeve po vepron në përputhje me ligjin dhe kërkon vetëm të dhënat e nevojshme për përmbushjen e kërkesës për rimbursim.
- **Kërkesa për fshirjen e të dhënave të panevojshme:** Në rast se të dhënat gjenetike janë mbledhur pa arsye të qartë ose pa pëlqimin e tij, Arbeni ka të drejtë të **kërkojë fshirjen e të dhënave të panevojshme** sipas **nenit 16**. Kjo përfshin kërkesën që të dhënat e ndjeshme të fshihen menjëherë nga sistemi i kompanisë së sigurimeve nëse ato janë mbledhur pa bazë ligjore.
- **Paraqitja e një ankese tek Agjencia:** Nëse Arbeni ndien se të dhënat e tij po përpunohen në mënyrë të paligjshme ose pa pëlqimin e tij të qartë, ai ka të drejtë të **paraqesë një ankesë në Agjencinë për Informim dhe Privatësi**, bazuar në **nenin 52**. Agjencia mund të hetojë rastin dhe të marrë masa për mbrojtjen e të drejtave të tij.
- **Kërkesa për dëmshpërblim:** Nëse kompania e sigurimeve përpunon të dhënat e tij pa justifikim ose i shkakton dëm Arbenit përmes trajtimit të paligjshëm të të dhënave të tij, ai ka të drejtë të **kërkojë dëmshpërblim** për shkeljen e të drejtave të tij, në përputhje me **nenin 56**.

SKENARI 5:

**Vendosja e
kamerave të
mbikëqyrjes nga
institucionet
publike dhe
private**

Respektimi i privatësisë
dhe mbrojtja e të dhënave
personale janë të drejta
të patjetërsueshme të çdo
punëtori në vendin e punës!



SKENARI 5:

Vendosja e kamerave të mbikëqyrjes nga institucionet publike dhe private



Blerina punon si asistente administrative në një zyrë shtetërore në Prizren. Së fundmi, kamerat u instaluan në të gjithë vendin e punës, duke përfshirë hapësirat e përbashkëta dhe dhomat e përbashkëta të pushimit (kuzhina që përdorej për drekë). Mbikëqyrja e vazhdueshme e bën Blerinën dhe kolegët e saj të ndihen në siklet, pasi ata po vëzhgoheshin edhe gjatë pushimeve të tyre. Punëtorët nuk u informuan për kamerat apo qëllimin e inçizimeve, duke ngritur shqetësime serioze për privatësinë në vendin e punës dhe të drejtat e punëtorëve në sektorin publik të Kosovës.

Obligimet e institucionit në rastin konkret:

Bazuar në **Ligjin për Mbrojtjen e të Dhënave Personale**, institucioni publik apo privat ka këto detyrime specifike për instalimin dhe menaxhimin e kamerave të mbikëqyrjes:

- 1 Vendimi i brendshëm për instalimin e kamerave:** Institucioni është i detyruar të marrë një vendim të brendshëm, i cili duhet të përmbajë arsyet për vendosjen e sistemeve të mbikëqyrjes me kamerë dhe personin përgjegjës për administrimin e tyre. Vendimi duhet të jetë në përputhje me **nenin 76**, i cili kërkon që mbikëqyrja të bëhet vetëm nëse është e nevojshme për sigurinë e njerëzve dhe të pronës dhe këto pamje nuk mund të përdoren për qëllime të tjera përveç nëse një gjë e tillë kërkohet nga një ligj i veçantë.
- 2 Njoftimi për vendosjen e kamerave:** Institucioni duhet të njoftojë qartë dhe në mënyrë të dukshme punonjësit për ekzistencën e kamerave dhe qëllimin e tyre, siç përcaktohet nga **neni 75, paragrafi 2** dhe **neni 78, paragrafi 4**. Njoftimi duhet të jetë i qartë dhe i dukshëm për të gjitha palët e përfshira, në mënyrë që të respektohen të drejtat e subjekteve të të dhënave.
- 3 Kufizimi i mbikëqyrjes:** Sipas **nenit 78, paragrafi 3**, vëzhgimi me kamerë ndalohet në hapësirat private, si dhomat e ndërrimit, kuzhinat, hapësirat sanitare, apo çdo hapësirë tjetër ku punonjësit kanë pritshmëri për privatësi. Vëzhgimi duhet të kufizohet vetëm në hapësirat ku rreziku i sigurisë është i pranishëm.
- 4 Ruajtja dhe mbrojtja e të dhënave:** Institucioni duhet të caktojë një periudhë maksimale për ruajtjen e regjistrimeve, që nuk mund të kalojë një muaj, përveç nëse ekzistojnë arsye legjitime për zgjatjen e këtij afati, sipas **nenit 76, paragrafi 7**. Të dhënat duhet të mbrohen nga qasja ose përdorimi i paautorizuar, **sipas nenit 75, paragrafi 4**.

Çka mund të bënte Blerina në rastin konkret?

Në bazë të **Ligjit për Mbrojtjen e të Dhënave Personale**, Blerina mund të ndër-marrë veprimet e mëposhtme për të mbrojtur privatësinë e saj:

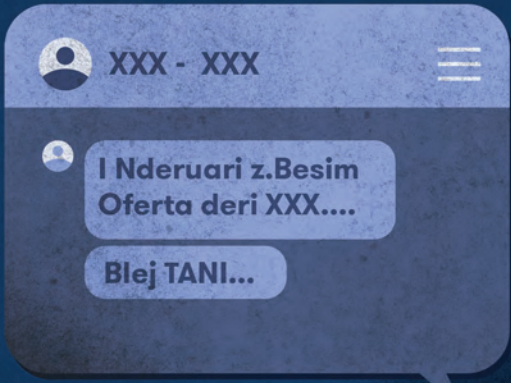
- 1 **Kërkesë për informim dhe transparencë:** Blerina ka të drejtë të kërkojë nga institucioni informacione të qarta mbi qëllimin e instalimit të kamerave, vendet ku janë vendosur dhe afatin e ruajtjes së të dhënave. Kjo kërkesë mbështetet nga **neni 14** i Ligjit.
- 2 **Kërkesë për ndërprerjen e përpunimit të të dhënave në hapësira private:** Nëse kamerat janë vendosur në hapësira të përbashkëta si kuzhina apo dhomat e pushimit, Blerina ka të drejtë të kërkojë ndërprerjen e përpunimit të të dhënave në këto hapësira private, sipas **nenit 78, paragrafi 3**.
- 3 **Ankesë tek Agjencia për Informim dhe Privatësi:** Nëse institucioni nuk vepron në përputhje me kërkesat e saj, Blerina ka të drejtë të paraqesë një ankesë tek Agjencia për Informim dhe Privatësi për hetim, sipas **nenit 52**.
- 4 **Kërkesë për fshirjen e të dhënave personale:** Blerina mund të kërkojë që të dhënat e saj të fshihen nëse janë përpunuar në mënyrë të paautorizuar ose në hapësira ku nuk duhet të ketë mbikëqyrje, në përputhje me **nenin 16** të Ligjit.
- 5 **Padi për kompensim të dëmeve:** Nëse Blerina vuan dëme materiale ose jomateriale për shkak të vendosjes së paligjshme të kamerave dhe mbikëqyrjes së privatësisë së saj, ajo ka të drejtë të kërkojë kompensim për dëmet e shkaktuara, në përputhje me **nenin 56**.

Këto veprime janë në përputhje me dispozitat ligjore dhe ndihmojnë Blerinën të mbrojë privatësinë dhe të drejtat e saj në vendin e punës.

SKENARI 6:

**Përpunimi i të
dhënave nga
institucionet
publike dhe
private të
telekomunikacionit**

Çdo informacion ka vlerë
- mbrojini ato si gjëra të
çmuara!



SKENARI 6:

Përpunimi i të dhënave nga institucionet publike dhe private të telekomunikacionit



Besimi, një 40-vjeçar nga Mitrovica, fillon të marrë oferta promovuese të personalizuar me SMS bazuar në historikun e tij të thirrjeve dhe historikun e shfletimit të internetit. Ai kurrë nuk ra dakord që të dhënat e tij të përdoren në këtë mënyrë dhe ndien se privatësia e tij është shkelur. Pas një hetimi, Besimi zbulon se ofruesi i tij i telekomunikacionit ka ndarë të dhënat e tij personale me firma të marketingut të palëve të treta pa pëlqimin e tij, një praktikë që nxjerr në pah mungesën e masave për mbrojtjen e të dhënave në sektorin e telekomunikacionit në Kosovë.

Obligimet e ofruesit të shërbimeve të telekomunikacionit në rastin konkret:

Bazuar në **nenin 73 të Ligjit për Mbrojtjen e të Dhënave Personale**, institucioni i telekomunikacionit ka detyrime specifike për përpunimin dhe ndarjen e të dhënave personale për qëllime të marketingut të drejtpërdrejtë. Këto detyrime përfshijnë:

- 1 Përdorimi i të dhënave vetëm me pëlqimin e qartë:** Institucioni i telekomunikacionit mund të përdorë vetëm të dhënat personale të grumbulluara nga burime publike ose të grumbulluara brenda aktiviteteve ligjore për qëllime të marketingut të drejtpërdrejtë, në përputhje me **nenin 73, paragrafi 1. Pëlqimi paraprak** është i domosdoshëm për të dhënat e tjera, veçanërisht ato të ndjeshme, të cilat mund të përpunohen vetëm me **pëlqimin e shprehur me shkrim**.
- 2 Informimi i subjektit të të dhënave për të drejtat e tij:** Në rast të marketingut të drejtpërdrejtë, institucioni ka detyrim t'i informojë subjektet e të dhënave, si Besimi, për të drejtat e tyre në përputhje me dispozitat e ligjit, duke përfshirë të drejtën për të kundërshtuar përpunimin e të dhënave personale për marketing, sipas **nenit 73, paragrafi 3**.
- 3 Zbulimi i të dhënave për palët e treta për qëllime marketingu:** Para se të ndahen të dhënat personale me palët e treta për qëllime marketingu, institucioni është i detyruar të marrë **pëlqimin e shprehur me shkrim** të Besimit. Për më tepër, institucioni duhet ta informojë atë për të gjitha informacionet që synohen të ndahen dhe me kë, në përputhje me **nenin 73, paragrafi 4**.
- 4 Kufizimi i përpunimit të të dhënave:** Institucioni mund të përpunojë për marketing të drejtpërdrejtë vetëm të dhënat bazë, si emri, adresa, numri i telefonit, dhe e-mail, dhe vetëm nëse Besimi ka dhënë pëlqimin e tij paraprak për përpunimin e këtyre të dhënave, në përputhje me **nenin 73, paragrafi 2**.

Çka mund të bënte Besimi në rastin konkret?

Në bazë të Ligjit për Mbrojtjen e të Dhënave Personale, Besimi mund të ndër marrë veprimet e mëposhtme për të mbrojtur të dhënat e tij personale dhe privatësinë:

- 1 **Kërkesë për ndërprerjen e përpunimit të të dhënave për marketing të drejtpërdrejtë:** Besimi mund të kërkojë që të ndërpritet përpunimi i të dhënave të tij për qëllime marketingu pa pëlqimin e tij të qartë, në përputhje me **nenin 20** të Ligjit, që i lejon të kundërshtojë përpunimin për marketing të drejtpërdrejtë.
- 2 **Kërkesë për fshirjen e të dhënave personale:** Nëse Besimi nuk ka dhënë pëlqimin e tij për përpunimin e të dhënave për marketing, ai mund të kërkojë që të dhënat e tij të fshihen nga të gjitha regjistrat e kompanive që i kanë marrë ato pa autorizimin e tij, sipas **nenit 16** të Ligjit.
- 3 **Kërkesë për transparencë dhe qasje në të dhëna:** Besimi mund të kërkojë informacione të qarta nga institucioni i telekomunikacionit për mënyrën se si janë përpunuar të dhënat e tij, burimet e grumbullimit të këtyre të dhënave dhe me cilat palë të treta janë ndarë, në përputhje me **nenin 14** të Ligjit.
- 4 **Kërkesë për pëlqimin e shkruar:** Nëse institucioni ka ndarë të dhënat e tij me palë të treta për marketing, Besimi ka të drejtë të kërkojë që të gjitha ndarjet e mëtejshme të dhënave të bëhen vetëm pas marrjes së pëlqimit të tij me shkrim, sipas **nenit 73, paragrafi 4**.
- 5 **Ankesë tek Agjencia për Informim dhe Privatësi:** Besimi mund të paraqesë një ankesë tek Agjencia për Informim dhe Privatësi nëse beson se të dhënat e tij janë përdorur në mënyrë të paligjshme pa pëlqimin e tij, sipas **nenit 52**.
- 6 **Padi për kompensim të dëmeve:** Nëse Besimi ka pësuar dëme materiale apo jomateriale si rezultat i përdorimit të paautorizuar të të dhënave të tij, ai ka të drejtë të kërkojë kompensim për dëmet e shkaktuara, në përputhje me **nenin 56** të Ligjit.

Këto veprime do të ndihmojnë Besimin të mbrojë të drejtat e tij për privatësi dhe të sigurojë që të dhënat e tij personale të mos përdoren në mënyrë të paligjshme nga institucionet e telekomunikacionit dhe palët e treta të përfshira në marketing.

SKENARI 7:

**Përdorimi i
kamerave dhe
përpunimi i të
dhënave në
institucionet
parashkollore**

Privatësia e fëmijëve është
një e drejtë thelbësore.
Të sigurojmë se të dhënat
e tyre mbrohen dhe se ata
rriten në një ambient të
sigurt!



SKENARI 7:

Përdorimi i kamerave dhe përpunimi i të dhënave në institucionet parashkollore



Drita, një vajzë 3-vjeçare, është dërguar nga prindërit e saj në një çerdhe në Ferizaj, ku kamera mbikëqyrjeje janë instaluar në klasa dhe në hapësirat e lojës. Çerdhja shpesh poston video dhe foto të fëmijëve në faqen e saj në Facebook për të treguar aktivitetet e përditshme. Prindërit e Dritës nuk u pyetën kurrë për pëlqim dhe mbetën të shokuar kur panë imazhet e vajzës së tyre në internet, të qasshme për tu parë për këdo. Ky skenar demonstroi shqetësimet në rritje të privatësisë lidhur me përdorimin e mbikëqyrjes në mjediset arsimore në Kosovë, veçanërisht kur përfshihen fëmijët.

Obligimet e çerdhes në rastin konkret:

Bazuar në **Ligjin për Mbrojtjen e të Dhënave Personale** dhe në veçanti në dispozitat për mbikëqyrjen me kamera dhe mbrojtjen e të dhënave të fëmijëve, çerdhja ka këto obligime specifike në lidhje me përdorimin e kamerave dhe përpunimin e të dhënave personale të fëmijëve:

- 1 Vendosja e njoftimeve për kamerat:** Çerdhja është e detyruar të vendosë njoftime të dukshme dhe të qarta në lidhje me përdorimin e kamerave, siç përcaktohet nga **neni 75, paragrafi 2**. Njoftimi duhet të jetë i qartë dhe i dukshëm, duke informuar prindërit dhe vizitorët për ekzistencën e kamerave dhe qëllimin e mbikëqyrjes.
- 2 Kërkimi i pëlqimit nga prindërit:** Duke qenë se mbikëqyrja me kamerë ndodh në hapësira ku përfshihen fëmijët, çerdhja duhet të marrë pëlqimin e shprehur me shkrim nga prindërit ose kujdestarët ligjorë të fëmijëve, në përputhje me **nenin 7 dhe nenin 73** të Ligjit. Pa pëlqimin e tyre, përpunimi i të dhënave vizuale për qëllime si publikimi në rrjetet sociale është i paligjshëm.
- 3 Përdorimi i kufizuar i kamerave:** Kamerat mund të instalohen vetëm në hapësirat ku është e nevojshme për sigurinë e njerëzve dhe pronës, si hyrjet dhe korridoret, sipas **nenit 76**. Vendosja e kamerave në klasat e fëmijëve ose në hapësirat e lojës duhet të shmanget për të mbrojtur privatësinë e fëmijëve.
- 4 Ruajtja e të dhënave:** Regjistrimet nga kamerat duhet të ruhen vetëm për aq kohë sa është e nevojshme për qëllimet e synuara dhe të mbrohen nga qasja dhe përdorimi i paautorizuar, sipas **nenit 75, paragrafi 4** dhe **nenit 76, paragrafi 6**. Ruajtja e të dhënave për më shumë se një muaj është e lejuar vetëm nëse ekziston një qëllim legjitim.
- 5 Informimi i prindërve dhe punonjësve të çerdhes për të drejtat e tyre:** Çerdhja duhet të informojë prindërit për të drejtat e tyre në lidhje me përpunimin e të dhënave personale të fëmijëve, përfshirë të drejtën për qasje, korrigjim, fshirje dhe kufizim të përpunimit, sipas **nenit 14** dhe punonjësit e çerdhes sipas **nenit 78, paragrafi 4**.

Çka mund të bënin prindërit e Dritës në rastin konkret?

Në bazë të **Ligjit për Mbrojtjen e të Dhënave Personale**, prindërit e Dritës mund të ndërmarrin veprimet e mëposhtme për të mbrojtur privatësinë e vajzës së tyre:

- 1 Kërkesë për informim dhe qartësim mbi përdorimin e kamerave:** Prindërit kanë të drejtë të kërkojnë që çerdhja t'i informojë për qëllimin dhe vendosjen e kamerave, si dhe për mënyrën se si përpunohen dhe ruhen të dhënat e fëmijëve të tyre. Ky veprim është mbështetur nga **neni 75** dhe **neni 14** i Ligjit.
- 2 Kundërshtimi i përpunimit të të dhënave për qëllime të padëshiruara:** Prindërit mund të kundërshtojnë përpunimin e të dhënave të fëmijës së tyre për publikim në rrjete sociale ose për qëllime marketingu, në përputhje me **nenin 20**, që i lejon subjektet e të dhënave të refuzojnë përpunimin për qëllime specifike.
- 3 Kërkesë për fshirjen e të dhënave personale:** Nëse video ose foto të fëmijës janë publikuar pa pëlqimin e tyre, prindërit kanë të drejtë të kërkojnë fshirjen e menjëhershme të materialeve nga të gjitha platformat ku janë publikuar, në përputhje me **nenin 16** të Ligjit.
- 4 Ankesë tek Agjencia për Informim dhe Privatësi:** Prindërit mund të paraqesin një ankesë tek Agjencia për Informim dhe Privatësi nëse ndiejnë se të dhënat e vajzës së tyre janë përpunuar në mënyrë të paligjshme, duke kërkuar marrjen e masave për mbrojtjen e të dhënave, në përputhje me **nenin 52**.
- 5 Padi për kompensim të dëmeve:** Nëse prindërit besojnë se vajza e tyre ka pësuar dëme materiale ose jomateriale për shkak të publikimit të paautorizuar të të dhënave të saj, ata mund të kërkojnë kompensim për dëmet e shkaktuara, sipas **nenit 56** të Ligjit.

Këto veprime sigurojnë që çerdhja të respektojë të drejtat e prindërve dhe të fëmijëve për mbrojtjen e të dhënave personale, duke përfshirë transparencën dhe sigurinë e regjistrimeve.

SKENARI 8:

**Përdorimi i
kamerave dhe
përpunimi i të
dhënave në
institucionet
shkollore**

Në institucionet
arsimore, nxënësit duhet
të aftësohen, jo t'ë
ekspozohen ndaj rreziqeve!



SKENARI 8:

Përdorimi i kamerave dhe përpunimi i të dhënave në institucionet shkollore



Arditi, një nxënës 16-vjeçar i shkollës së mesme në Gjakovë, është filmuar nga kamera për mbikqyrje, e instaluar në klasën e tij. Pamjet ruhen në serverin e shkollës, por masat e sigurisë janë të dobëta dhe disa anëtarë të stafit kanë akses të pakufizuar. Një ditë, një mësues aksidentalisht ndan një video klip të Arditi duke u pyetur në lëndën e biologjisë, në një grup të stafit në Viber, duke ekspozuar atë pa pëlqim. Arditi ka një gjendje të vështërsisë në të shprehur, sidomos nën situatat në tension. Videoja e qarkulluar në grupin e Viber-it, qarkullon edhe jashtë tij dhe postohet nga palët e treta edhe në rrjetin Facebook dhe Instagram. Arditi e përjeton rëndë këtë situatë dhe kërkon ndërrimin e shkollës.

Obligimet e shkollës në rastin konkret:

Bazuar në **Ligjin për Mbrojtjen e të Dhënave Personale**, si dhe në dispozitat specifike për përdorimin e kamerave në sektorin e arsimit, shkolla ka këto detyrime në lidhje me mbikëqyrjen me kamera dhe përpunimin e të dhënave personale të nxënësve:

- 1 Vendimi i brendshëm për instalimin e kamerave:** Shkolla është e detyruar të marrë një **vendim të brendshëm** për instalimin e kamerave, i cili duhet të përfshijë **qëllimin e qartë** të përdorimit të kamerave dhe **personin përgjegjës** për administrimin e tyre, sipas **nenit 76, paragrafi 2**. Ky vendim duhet të justifikojë nevojën e instalimit të kamerave në hapësira si klasat e mësimit.
- 2 Njoftimi për përdorimin e kamerave:** Nxënësit, prindërit dhe stafi i shkollës duhet të informohen qartë dhe me shkrim për ekzistencën e kamerave dhe qëllimin e tyre, sipas **nenit 75, paragrafi 2** dhe **nenin 78, paragrafi 4**. Njoftimet duhet të jenë të dukshme në të gjitha hapësirat ku ka kamera.
- 3 Ruajtja dhe siguria e të dhënave:** Të dhënat e mbledhura përmes kamerave duhet të ruhen në mënyrë të sigurt dhe të mbrohen nga qasja e paautorizuar. Në këtë rast, **accesi i pakufizuar i disa anëtarëve të stafit** në të dhënat e ruajtura është në kundërshtim me **nenin 75, paragrafi 4**, i cili kërkon që të dhënat të mbrohen nga përdorimi i paautorizuar. Ruajtja e të dhënave duhet të jetë e kufizuar në periudhën që është e nevojshme për qëllimin e përpunimit, në përputhje me **nenin 76, paragrafi 7**.
- 4 Kufizimi i përpunimit të të dhënave:** Shkolla duhet të kufizojë përpunimin e pamjeve vetëm për qëllime të sigurisë dhe nuk duhet të ndodhë shpërndarja e tyre pa **pëlqimin e shprehur** të nxënësve ose prindërve, veçanërisht në situata ku publikimi i pamjeve shkakton dëm. Ndërprerja e shpërndarjes pa leje është e kërkuar nga **neni 73, paragrafi 4**.
- 5 Pëlqimi i nxënësit ose prindërve:** Për nxënësit nën 16 vjeç, pëlqimi për përpunimin e të dhënave personale duhet të jepet nga prindërit ose kujdestarët, sipas **nenit 7**. Në këtë rast, Arditi është mbi 16 vjeç dhe duhet të ketë dhënë pëlqimin e tij për përpunimin dhe përdorimin e pamjeve të tij në çfarëdo formë, veçanërisht për publikim të mëtejshëm.
- 6 Trajnimi i stafit:** Shkolla është e detyruar të informojë dhe trajnojë stafin për **përgjegjësitë e tyre** në lidhje me mbrojtjen e të dhënave personale të nxënësve dhe përdorimin e duhur të kamerave.

Çka mund të bënte Arditi apo familja e tij në rastin konkret?

Bazuar në **Ligjin për Mbrojtjen e të Dhënave Personale**, Arditi dhe prindërit e tij mund të ndër marrin veprimet e mëposhtme për të mbrojtur të drejtat e tij:

- 1 **Kërkesë për informim mbi përdorimin e kamerave:** Arditi dhe prindërit e tij kanë të drejtë të kërkojnë informacion mbi **qëllimin dhe vendosjen e kamerave** në klasë, si dhe masat e sigurisë që shkolla ka marrë për ruajtjen e të dhënave, sipas **nenit 14**. Ata mund të kërkojnë gjithashtu qasje në të dhënat e mbledhura për Arditin.
- 2 **Kërkesë për fshirjen e të dhënave:** Arditi ka të drejtë të kërkojë **fshirjen e menjëhershme** të të dhënave të tij personale që janë përpunuar dhe shpërndarë pa pëlqimin e tij, veçanërisht pamjet që janë shpërndarë në Viber dhe rrjete sociale, sipas **nenit 16** të Ligjit.
- 3 **Kundërshtimi i përpunimit të të dhënave:** Arditi mund të kundërshtojë përpunimin e mëtejshëm të të dhënave të tij personale dhe të kërkojë ndërprerjen e mbikëqyrjes së paautorizuar në klasë ose kufizimin e përpunimit, sipas **nenit 20** të Ligjit.
- 4 **Ankesë tek Agjencia për Informim dhe Privatësi:** Nëse shkolla nuk përmbush kërkesat për mbrojtjen e të dhënave personale, Arditi dhe prindërit e tij mund të paraqesin një ankesë tek Agjencia për Informim dhe Privatësi, duke kërkuar marrjen e masave të nevojshme për mbrojtjen e të dhënave të tij, sipas **nenit 52**.
- 5 **Kërkesë për kompensim të dëmeve:** Nëse shpërndarja e pamjeve ka shkaktuar dëme psikologjike dhe emocionale për Arditin ai ose prindërit e tij kanë të drejtë të kërkojnë **kompensim për dëmet materiale dhe jomateriale**, sipas **nenit 56** të Ligjit.

Përmirësimet për masat mbrojtëse të shkollës:

Bazuar në Ligjin për Mbrojtjen e të Dhënave Personale, Arditi dhe prindërit e tij mund të ndërmarrin veprimet e mëposhtme për të mbrojtur të drejtat e tij:

- 1 Instalimi i kamerave duhet të kufizohet vetëm në hapësira ku ka nevojë për siguri**, si hyrjet apo korridoret, dhe jo në klasat e mësimit ku nxënësit janë të ekspozuar ndaj filmimit të pandërprerë, sipas **nenit 78, paragrafi 2**.
- 2 Sistemet e sigurisë së serverëve duhet të përmirësohen**, dhe qasja në regjistrime duhet të jetë e kufizuar dhe monitoruar, duke siguruar që vetëm personeli i autorizuar të ketë akses në të dhënat e mbledhura, sipas **nenit 75, paragrafi 4**.

Këto masa do të ndihmojnë në sigurimin e mbrojtjes së të drejtave të Arditi dhe do të sigurojnë që përpunimi i të dhënave të jetë i ligjshëm dhe në përputhje me standardet për mbrojtjen e privatësisë.

SKENARI 9:

**Marketingu i
drejtpërdrejtë -
SMS dhe thirrje
telefonike të
pandërprera**

Çdo informatë personale
është pjesë e identitetit
tonë - mbrojtja e saj është
detyrim për çdo kompani
dhe institucion!



SKENARI 9:

Marketingu i drejtpërdrejtë - SMS dhe thirrje telefonike të pandërprera



Valbona, një pensioniste 62-vjeçare nga Prishtina, fillon të marrë thirrje të pandërprera dhe mesazhe SMS nga një kompani e re farmaceutike që promovon produktet e caktuara mjeksësore. Ajo është e habitur pasi kurrë nuk i ka dhënë të dhënat e saj kontaktuese kësaj kompanie. Për më tepër ajo habitet sepse ofertat që Valbona pranon janë pikërisht për sëmundjen dhe shqetësimet shëndetësore që ajo ka identifikuar së fundi. Del që të dhënat e saj janë shitur nga një agjenci marketingu e palës së tretë pa dijeninë e saj, duke shkaktuar shqetësim dhe duke nxjerrë në pah natyrën ndërhyrëse të praktikave të marketingut të drejtpërdrejtë në Kosovë, të cilat shpesh ndodhin pa mbrojtje të mjaftueshme të konsumatorëve.

Obligimet e kompanisë farmaceutike dhe agjencisë së marketingut në rastin konkret:

Bazuar në **Ligjin për Mbrojtjen e të Dhënave Personale**, dhe në veçanti dispozitat për **marketingun e drejtpërdrejtë**, kompania farmaceutike dhe agjencia e marketingut kanë disa detyrime specifike për të mbrojtur të dhënat personale të Valbonës dhe për të siguruar që praktikrat e tyre janë në përputhje me ligjin:

- 1 Kërkimi i pëlqimit të qartë dhe të informuar:** Kompania farmaceutike dhe agjencia e marketingut janë të detyruara të marrin **pëlqimin e qartë dhe të informuar** të Valbonës për përpunimin dhe përdorimin e të dhënave të saj personale për qëllime të marketingut të drejtpërdrejtë, në përputhje me **nenin 73** të Ligjit. Pëlqimi duhet të përfshijë qartësisht se cilat të dhëna do të përdoren dhe për çfarë qëllimi, si dhe të informojë Valbonën për të drejtat e saj.
- 2 Përdorimi i të dhënave personale për marketing:** Në bazë të **nenit 73, paragrafi 2**, kontrolluesit e të dhënave mund të përdorin vetëm të dhënat personale që janë marrë ligjërisht për qëllime të marketingut të drejtpërdrejtë, si emri, adresa dhe numri i telefonit. Çdo përdorim i të dhënave të ndjeshme shëndetësore kërkon **pëlqimin e shprehur me shkrim** nga Valbona.
- 3 Ndalohet shpërndarja e të dhënave pa pëlqim:** Agjencia e marketingut nuk mund të shpërndajë të dhënat personale të Valbonës te kompanitë e tjera pa pëlqimin e saj të shprehur paraprakisht, sipas **nenit 73, paragrafi 4**. Kjo dispozitë kërkon që çdo zbulim i të dhënave të bëhet vetëm pas marrjes së pëlqimit dhe njoftimit të qartë për subjektin e të dhënave.
- 4 Masat e sigurisë për mbrojtjen e të dhënave:** Kompania farmaceutike dhe agjencia e marketingut duhet të sigurojnë që të dhënat e Valbonës janë të mbrojtura nga qasja e paautorizuar ose shpërndarja e paautorizuar, duke marrë **masa teknike dhe organizative** për të garantuar sigurinë e të dhënave, sipas **nenit 31** të Ligjit. Këto masa përfshijnë enkriptimin dhe pseudonimizimin e të dhënave personale, si dhe mbrojtjen nga çdo humbje ose asgjësim i paautorizuar.
- 5 Informimi për të drejtat:** Valbona duhet të informohet për të drejtat e saj për të kundërshtuar marketingun e drejtpërdrejtë, sipas **nenit 73, paragrafi 3**, që përfshin të drejtën për të refuzuar përpunimin e të dhënave për qëllime të marketingut dhe të kërkojë që të mos kontaktohet më përmes telefonatave ose SMS-ve.

Çka mund të bënte Valbona në rastin konkret?

Në bazë të **Ligjit për Mbrojtjen e të Dhënave Personale**, Valbona mund të ndërmarrë veprimet e mëposhtme për të mbrojtur të drejtat e saj:

- 1 **Kërkesë për fshirjen e të dhënave personale:** Valbona ka të drejtë të kërkojë fshirjen e të dhënave personale të saj që janë përpunuar pa pëlqimin e saj dhe të ndalojë kompaninë farmaceutike dhe agjencinë e marketingut nga përpunimi i mëtejshëm i të dhënave të saj, në përputhje me **nenin 16** të Ligjit.
- 2 **Kundërshtimi i marketingut të drejtpërdrejtë:** Valbona mund të kundërshtojë përpunimin e të dhënave të saj për qëllime të marketingut të drejtpërdrejtë dhe të kërkojë që të mos kontaktohet më nga kompania farmaceutike ose agjencia e marketingut, në përputhje me **nenin 20** dhe **nenin 74**.
- 3 **Kërkesë për informim dhe transparencë:** Valbona mund të kërkojë informacione mbi mënyrën se si të dhënat e saj janë përpunuar dhe ndarë me palët e treta, duke u bazuar në **nenin 14**. Ajo ka të drejtë të dijë se si janë marrë të dhënat e saj dhe kush ka qasje në to.
- 4 **Ankesë tek Agjencia për Informim dhe Privatësi:** Nëse Valbona beson se të dhënat e saj janë përpunuar në mënyrë të paligjshme, ajo ka të drejtë të paraqesë një ankesë tek Agjencia për Informim dhe Privatësi, në përputhje me **nenin 52** të Ligjit. Agjencia mund të hetojë çështjen dhe të marrë masat e nevojshme për mbrojtjen e të dhënave të saj.
- 5 **Padi për kompensim të dëmeve:** Nëse Valbona beson se ka pësuar dëme materiale ose jomateriale për shkak të shpërndarjes së paautorizuar të të dhënave të saj, ajo mund të kërkojë kompensim për dëmet e shkaktuara, sipas **nenit 56** të Ligjit.

Masa shtesë që duhet të ndërmarrë kompania farmaceutike:

Bazuar në Ligjin për Mbrojtjen e të Dhënave Personale, Arditi dhe prindërit e tij mund të ndërmarrin veprimet e mëposhtme për të mbrojtur të drejtat e tij:

- 1 Kërkimi dhe verifikimi i pëlqimit të subjekteve të të dhënave:** Kompania duhet të sigurohet që të marrë pëlqimin paraprak të Valbonës për përdorimin e të dhënave të saj personale për qëllime të marketingut, siç përcaktohet në **nenin 73, paragrafi 1**.
- 2 Ruajtja dhe mbrojtja e të dhënave:** Kompania duhet të zbatojë masa të përshtatshme teknike dhe organizative për të mbrojtur të dhënat e Valbonës nga qasja dhe shpërndarja e paautorizuar, siç kërkohet në **nenin 31**.
- 3 Transparenca dhe informimi:** Kompania duhet të sigurojë që Valbona të jetë plotësisht e informuar për mënyrën se si të dhënat e saj personale do të përpunohen dhe për të drejtat e saj për të kundërshtuar përpunimin për qëllime marketingu, sipas **nenit 14** dhe **nenit 73, paragrafi 3**.

Këto masa do të sigurojnë që të dhënat personale të Valbonës janë përpunuar në mënyrë të ligjshme dhe në përputhje me standardet për mbrojtjen e privatësisë.

SKENARI 10:

**Transferimi
i të dhënave
personale nga
bankat**

E drejta për privatësi është
gurëthemel i një shoqërie
demokratike – është
përgjegjësi e të gjithëve
që ta mbrojmë atë me çdo
çmim!



CREDIT CARD
1234 5678 9012 3456
Agon Banka

SKENARI 10:

Transferimi i të dhënave personale nga bankat



Agoni, një 27-vjeçar profesionist i IT-së, hap një llogari të re bankare në një bankë të njohur në Prishtinë. Banka e informon atë se të dhënat e tij personale dhe financiare do të ruhen nga një ofrues shërbimesh të palës së tretë jashtë vendit. Pa pëlqimin e qartë të Agonit, të dhënat e tij transferohen më pas te një kompani tjetër si pjesë e një marrëveshjeje të re shërbimi. Ndërkohë kompania në të cilën ruheshin të dhënat e tij jashtë vendit, për shkak të politikave të dobëta të atij vendi, i shiti të dhënat e 100,000 personave, përfshirë edhe ato të Agonit, tek një palë e tretë. Pala e tretë pastaj e kuptoj gjendjen financiare të Agonit dhe anuloi një marrëveshje që ishte në negociim e sipër për shitblerjen e disa aksioneve sepse duke kuptuar gjendjen financiare të Agonit pala e tretë kërkonte një çmim shumë herë më të lartë se ai për të cilin kishte filluar negociimi.

Agoni ndihet se privatësia e tij është shkelur, pasi informacioni i tij i ndjeshëm po transferohet midis kompanive të shumta pa njoftim të duhur, duke nxjerrë në pah mungesën e transparencës se si bankat në Kosovë trajtojnë të dhënat personale.

Obligimet e bankës dhe palës së tretë në rastin konkret:

Në bazë të **Ligjit për Mbrojtjen e të Dhënave Personale**, banka dhe ofruesit e shërbimeve të palës së tretë jashtë vendit kanë disa obligime kyçe për të siguruar që të dhënat personale të Agonit trajtohen me transparencë dhe siguri të mjaftueshme:

- 1 Njoftimi dhe kërkimi i pëlqimit të qartë:** Në përputhje me **nenin 14 dhe 49** të Ligjit, banka duhet të informojë Agonin në mënyrë të qartë dhe transparente për transferimin e të dhënave personale te ofruesi i shërbimeve jashtë vendit. Kjo duhet të përfshijë **qëllimin dhe mënyrën e përpunimit** të të dhënave dhe pëlqimi i Agonit duhet të merret për këtë transferim, nëse transferimi nuk është i detyrueshëm sipas një ligji apo traktati ndërkombëtar.
- 2 Niveli i mbrojtjes në vendin e tretë: Neni 44 dhe 45** theksojnë se transferimi i të dhënave personale jashtë vendit mund të bëhet vetëm nëse vendi pranues siguron një **nivel të duhur të mbrojtjes** së të dhënave personale, i përcaktuar nga **Agjencia për Informim dhe Privatësi**. Banka është e detyruar të verifikojë që vendi apo organizata pranues e të dhënave ofron **siguri të barabartë ose më të lartë** me standardet në Kosovë.
- 3 Sigurimi i masave teknike dhe organizative:** Banka dhe përpunuesi i të dhënave jashtë vendit janë të detyruar të zbatojnë **masa teknike dhe organizative të përshtatshme** për të mbrojtur të dhënat personale të Agonit, sipas **nenit 31**. Kjo përfshin **pseudonimizimin dhe enkriptimin** e të dhënave, si dhe aftësinë për të rivendosur disponueshmërinë e tyre në rast të ndonjë incidenti.

- 4** **Marrëveshja kontraktuale me përpunuesin e jashtëm:** Banka duhet të ketë një **marrëveshje të qartë kontraktuale** me përpunuesin e të dhënave jashtë vendit, e cila përfshin detajet për sigurinë e të dhënave dhe garancitë për përpunimin e tyre, në përputhje me **nenin 47 , paragrafi 1**. Kjo marrëveshje duhet të përmbajë detaje për mbrojtjen e të dhënave dhe kufizimin e përdorimit të tyre për qëllime të tjera nga ato për të cilat janë transferuar.
- 5** **Njoftimi për çdo rrjedhje të të dhënave:** Në rast të një **rrjedhje të të dhënave** nga pala e tretë jashtë vendit, banka ka obligim të njoftojë **Agjencinë për Informim dhe Privatësi brenda 72 orëve** dhe të informojë klientët, përfshirë Agonin, për natyrën e rrjedhjes, në përputhje me **nenin 33** të Ligjit. Banka është përgjegjëse për të siguruar që përpunuesi jashtë vendit të përmbushë këto detyrime.
- 6** **Lista e vendeve me nivel të duhur të mbrojtjes:** Sipas **nenit 46**, Agjencia duhet të mbajë **një listë të vendeve ose organizatave ndërkombëtare** që sigurojnë një nivel të duhur të mbrojtjes së të dhënave. Banka është përgjegjëse për të siguruar që transferimi i të dhënave të Agonit është bërë vetëm në një vend që figuron në këtë listë, ose nëse jo, të sigurojë autorizimin nga Agjencia për transferimin e të dhënave në një vend të tretë me mbrojtje të pamjaftueshme.

Çka mund të bënte Agoni në rastin konkret?

Në bazë të **Ligjit për Mbrojtjen e të Dhënave Personale**, Agoni mund të ndër marrë veprimet e mëposhtme për të mbrojtur të drejtat e tij dhe për të kërkuar transparencë në lidhje me përpunimin e të dhënave të tij:

- 1 Kërkesë për informacion mbi transferimin e të dhënave:** Agoni ka të drejtë të kërkojë **informacion të qartë dhe të plotë** nga banka për arsyet e transferimit të të dhënave personale jashtë vendit, përfshirë masat mbrojtëse të marra nga përpunuesi jashtë vendit, në përputhje me **nenin 14**.
- 2 Kundërshtimi i përpunimit të mëtejshëm të të dhënave:** Agoni mund të **kundërshtojë përpunimin e mëtejshëm** të të dhënave të tij personale nga kompania jashtë vendit nëse ky përpunim është bërë pa pëlqimin e tij ose është në kundërshtim me qëllimin për të cilin të dhënat janë mbledhur, në përputhje me **nenin 20**.
- 3 Kërkesë për fshirjen e të dhënave personale:** Agoni ka të drejtë të kërkojë **fshirjen e të dhënave të tij personale** nga përpunuesi jashtë vendit dhe nga çdo palë e tretë që ka marrë qasje në këto të dhëna, në përputhje me **nenin 16** të Ligjit, sidomos në rast të shpërdorimit të të dhënave të tij për qëllime të tjera.
- 4 Ankesë tek Agjencia për Informim dhe Privatësi:** Nëse Agoni beson se të dhënat e tij janë transferuar dhe përpunuar në mënyrë të paligjshme, ai ka të drejtë të paraqesë një **ankesë tek Agjencia për Informim dhe Privatësi**, e cila mund të hetojë rastin dhe të vendosë për masat e nevojshme, sipas **nenit 52**.
- 5 Padi për kompensim të dëmeve:** Nëse Agoni ka pësuar dëme materiale ose jomateriale si rezultat i transferimit të paautorizuar të të dhënave të tij, ai ka të drejtë të kërkojë **kompensim për dëmet e shkaktuara**, në përputhje me **nenin 56**.

Masa shitesë që duhet të ndërmarrë banka dhe përpunuesi jashtë vendit:

- 1 Autorizimi i Agjencisë për transferimin:** Nëse vendi ose organizata e huaj nuk figuron në listën e vendeve me **mbrojtje të mjaftueshme** të të dhënave, banka duhet të marrë një **autorizim nga Agjencia për Informim dhe Privatësi** për të realizuar transferimin, në përputhje me **nenin 49**.
- 2 Njoftimi për klientin:** Banka duhet të njoftojë Agonin për çdo **ndërhyrje të mëtejshme** në përpunimin e të dhënave të tij nga pala e tretë jashtë vendit, përfshirë ndarjen e të dhënave me palë të tjera, në përputhje me **nenin 45**.
- 3 Masat për mbrojtjen e të dhënave:** Banka dhe përpunuesi jashtë vendit duhet të implementojnë **masa adekuate teknike dhe organizative**, duke përfshirë **enkriptimin dhe pseudonimizimin** e të dhënave, për të garantuar që të dhënat e Agonit janë të sigurta dhe të mbrojtura nga çdo qasje e paautorizuar, në përputhje me **nenin 31**.

Këto masa dhe veprime do të sigurojnë që transferimi i të dhënave të Agonit të kryhet në përputhje me ligjin dhe të mbrojtë të drejtat e tij për privatësi dhe siguri të të dhënave personale.

Ky dokument është realizuar si pjesë e projektit "Human Rightivism", në kuadër të nismës "Gardianët e të dhënave: Forcimi i Politikave të Privatësisë dhe Ndërgjegjësimi në Institucionet Publike" që udhëhiqet nga Lëvizja FOL. Projekti implementohet nga Fondi për Zhvillim Komunitar (CDF) me mbështetjen e Ambasadës së Suedisë në Prishtinë.

