VENDIM
Nr. 151, **datë 11.3.2026**

PËR PËRCAKTIMIN E STANDARDEVE, QË KANË TË BËJNË ME KUSHTET TEKNIKE TË SISTEMIT TË BASTEVE SPORTIVE *ONLINE*, DUKE PËRFSHIRË, POR PA U KUFIZUAR, NË IDENTIFIKIMIN DHE REGJISTRIMIN E LOJTARËVE, KËRKESAT E PROGRAMEVE *SOFTWARE* DHE *HARDWARE*, CERTIFIKIMIN E SISTEMIT, PROCEDURAT LIDHUR ME FATURAT DHE TRANSAKSIONET E PAGESAVE, PARIMET E SIGURISË DHE KUSHTET E KONTROLLIT APO TË MBIKËQYRJES

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 2, të nenit 24, të ligjit nr. 155/2015, "Për lojërat e fatit në Republikën e Shqipërisë", të ndryshuar, me propozimin e ministrit të Financave, Këshilli i Ministrave

VENDOSI:

I. DISPOZITA TË PËRGJITHSHME

Ky vendim ka për qëllim përcaktimin e standardeve, që kanë të bëjnë me kushtet teknike dhe standardet minimale, që duhet të plotësojnë sistemet/*website*-t/aplikacionet e basteve sportive *online* të subjekteve të licencuara, të cilat konsistojnë në:

a) kërkesat teknike minimale, që duhet të plotësojnë sistemet, ku administrohen, menaxhohen dhe luhen bastet sportive *online*, duke përfshirë komponentët *hardware* dhe *software*;

b) kërkesat për identifikimin e regjistrimin e lojtarëve, me qëllim sigurimin e aksesit të ligjshëm, mbrojtjen e të dhënave dhe parandalimin e lojës së paligjshme;

c) procedurat në lidhje me faturat dhe transaksionet e pagesave, duke siguruar që çdo transaksion të regjistrohet e të monitorohet në kohë reale nga organet përkatëse;

ç) procedurat lidhur me faturat dhe transaksionet e pagesave;

d) certifikimin e sistemit.

II. KËRKESAT MINIMALE QË DUHET TË PËRMBUSHË PLATFORMA, KU DO TË ADMINISTROHEN, MENAXHOHEN DHE LUHEN BASTET SPORTIVE *ONLINE*

1. Sistemi qendror (*BackEnd*)

1.1. Arkitektura e përgjithshme

a) Sistemi duhet të ndërtohet bazuar në një arkitekturë me **mikroshërbime** për modularitet, shkallëzim e mirëmbajtje të lehtë;

b) Arkitektura e sistemit duhet të disponojë **shpërndarës ngarkese (*load balancer)*** për shpërndarjen e trafikut ndërmjet instancave të aplikacionit;

c) Arkitektura duhet të operojë, duke u bazuar në **ngjarje *(event-driven)*** për përpunimin e basteve "*live*" dhe të rezultateve në kohë reale;

ç) Arkitektura e sistemit duhet të disponojë shtresë **kujtese të përkohshme *(caching*)** për uljen e ngarkesës në bazën e të dhënave;

d) Arkitektura e sistemit duhet të ofrojë mundësi për **shkallëzim horizontal e vertikal**, në varësi të ngarkesës së përdoruesve.

1.2 Shërbimet kryesore:

a) Shërbimi i përdoruesve:

i. sistemi duhet të ketë të implementuar mekanizma, që mundësojnë regjistrimin, hyrjen *(login)* dhe menaxhimin e profileve të përdoruesve;

ii. sistemi duhet të ketë të implementuar mekanizma për autentifikimin dhe autorizimin me role (minimalisht duhet të përfshijë rolet: përdorues, operator, administrator, audites);

iii. sistemi duhet të ketë të implementuar mekanizma për gjurmim të çdo veprimi të përdoruesit dhe të mundësojë ruajtjet e historikut të veprimeve;

b) Shërbimi i basteve:

i. sistemi duhet të ofrojë mundësinë për krijim e përpunim bastesh të vetme dhe të shumëfishta;

ii. sistemi duhet të ketë të implementuar mekanizma kontrolli për kufijtë financiarë dhe rregullat e lojës;

iii. sistemi duhet të disponojë algoritme të posaçme për llogaritje të fitimeve;

iv. në rast se organizatori i licencuar do të implementojë algoritme të bazuara në inteligjencën artificiale për shërbimin e basteve, në çdo rast në ndërfaqen *web* dhe/ose aplikacionin për përdoruesit duhet të jetë e publikuar logjika e algoritmit të implementuar për arsye transparence. Në çdo rast, çdo mjet i inteligjencës artificiale, që do të implementohet, duhet të jetë në përputhje me përcaktimet ligjore në Republikën e Shqipërisë dhe *EU AI Act*;

v. sistemi duhet të mundësojë marrje të dhënash nga palë të treta, siç mund të jenë ofrues të shërbimeve të kuotimit të jashtëm;

vi. sistemi duhet të mundësojë përditësim në kohë reale të ngjarjeve dhe të rezultateve;

c) Raportim dhe analiza:

i. sistemi duhet të ofrojë raporte me të dhëna reale dhe **të azhurnuara** për aktivitetin financiar, përdoruesit, fitimet dhe ngjarjet e vendosura, **raporte të detajuara të bilancit të lojtarëve,** raporte të pagesave dhe të tërheqjeve;

ii. sistemi duhet të ketë mekanizma të integruar për monitorimin e raportimin e aktivitetit të bastit, duke përfshirë raportet e të ardhurave, transaksioneve, statistikat e lojërave, raportet e rrezikut, bonuseve dhe promocioneve, si dhe identifikimin e sjelljeve të pazakonta të përdoruesve;

iii. raportimi duhet të përfshijë të ardhurat bruto nga bastet, fitimet neto, numrin e basteve të vendosura dhe raportet e dyshimeve për pastrim parash apo aktivitet të parregullt;

iv. sistemi duhet të sigurojë raportimin automatik për nevojat e rregullatorit. Kjo përfshin raportimin e transaksioneve të dyshimta dhe basteve të dyshimta, raportimin e detyrimeve fiskale, si dhe mekanizma të mbrojtjes së lojtarëve, në përputhje me kuadrin ligjor të lojërave të fatit në Shqipëri;

ç) Sistemi duhet:

i. të jetë i aftë t'u ofrojë lojtarëve një histori të transaksioneve të lojërave;

ii. të jetë i aftë t'u ofrojë lojtarëve një histori të transaksioneve financiare, duke përfshirë totalin e depozitave, tërheqjeve, fitimeve/humbjeve dhe pozicionin neto total;

iii. të ofrojë informacion të detajuar për çdo lojë;

iv. të shfaqë emrin e çdo loje;

v. të komunikojë kufizimet në lojë;

vi. të ofrojë udhëzime mbi mënyrën e lojës;

vii. të ofrojë një tabelë pagesash për të gjitha shpërblimet dhe funksionet/skenarët e veçantë të lojës;

viii. të shfaqë bilancin aktual të llogarisë së lojtarit;

ix. të shfaqë në çdo kohë bilancin e llogarisë së lojtarit dhe monedhën përkatëse;

x. të japë informacion për mbrojtjen e lojtarit dhe rrezikun e lojërave të fatit;

d) Siguria:

i. sistemi duhet të mundësojë komunikim të sigurt me ***HTTPS/TLS 1.3*** **ose ekuivalent**;

ii. sistemi duhet të mundësojë kodim të fjalëkalimeve me ***bcrypt***, ***argon2***;

iii. sistemi duhet të ketë të implementuar mekanizma për menaxhimin e përdoruesve dhe të *logim*-it të tyre, sipas roleve (RBAC);

iv. sistemi duhet të ketë të implementuar mekanizma automatikë për kufizim të kërkesave për mbrojtje nga sulmet *DDoS* ose të ngjashme dhe validim të *login*-eve për mbrojtje nga *SQL Injection, XSS* ose të ngjashme;

v. Sistemi duhet të ketë të integruar mekanizma, që detyrojnë përdorimin e një niveli të lartë të kompleksitetit të fjalëkalimeve, të cilat duhet të plotësojnë minimalisht kushtet e mëposhtme:

- Fjalëkalimi duhet të jetë i përbërë nga të paktën 9 (nëntë) karaktere të kombinuara alfanumerike e speciale dhe janë miksim "*lowercase*" *dhe* "*uppercase*";
- Fjalëkalimi nuk duhet të jetë i njëjtë me emrin e llogarisë;
- Nëse fjalëkalimi ndryshohet, fjalëkalimi i ri duhet të jetë i ndryshëm nga të paktën 3 (tri) fjalëkalimet e fundit të përdorura për llogarinë.

1.3 Regjistrimi i përdoruesit, identifikimi dhe menaxhimi i llogarisë:

a) Sistemi duhet të ofrojë një proces të lehtë dhe të sigurt të regjistrimit të përdoruesit;

b) Sistemi duhet të ketë një modul të centralizuar për menaxhimin e identitetit e të aksesit;

c) Çdo përdorues, administrator, operator apo agjent duhet të ketë **identitet unik** dhe **kredenciale të personalizuara**;

ç) Sistemi duhet të zbatojë mekanizma bllokimi pas 5 (pesë) përpjekjeve të dështuara;

d) Sesionet e përdoruesit duhet të skadojnë automatikisht pas një periudhe mosveprimi nga përdoruesi. Kjo periudhë nuk duhet të jetë më e gjatë se 60 (gjashtëdhjetë) minuta;

dh) Sistemi nuk duhet të regjistrojë asnjë përdorues, nëse nuk janë vendosur të dhënat: emër, mbiemër, datëlindje, adresë, dokument identifikimi i skanuar, adresë *email*-i, numër telefoni. Në mënyrë që përdoruesi të konfirmohet dhe të ketë mundësinë të përdorë sistemin, duhet të kryhet verifikimi i tij nëpërmjet adresës së *email*-it ose numrit të telefonit të vendosur nga përdoruesi gjatë regjistrimit për të verifikuar identitetin e përdoruesit dhe për të minimizuar rrezikun e krijimit të llogarive të rreme;

e) Identifikimi bëhet me fjalëkalim të fortë, autentifikim me 2 (dy) faktorë dhe verifikim të moshës ligjore të përdoruesit;

ë) Sistemi duhet të ketë të integruar mekanizma të leximit të dokumentit të skanuar (dokument identifikimi) dhe, nëpërmjet tij, të sigurojë ligjshmërinë e përdoruesit për t'u regjistruar sipas moshës minimale të përcaktuar në legjislacionin shqiptar;

f) Në rast se zbulohet një aktivitet i dyshimtë ose i paautorizuar në llogarinë e një përdoruesi, duhet të ketë mekanizma për raportim e ndërhyrje të menjëhershme për të parandaluar shfrytëzimin e llogarisë dhe për të siguruar llogarinë e përdoruesit;

g) Në rast se në sistem do të aplikohen politika të çaktivizimit automatik të llogarive, ato nuk duhet të çaktivizohen në asnjë rast pa njoftuar përdoruesin të paktën 30 (tridhjetë) ditë përpara çaktivizimit të llogarisë;

gj) Përdoruesit nuk duhet të jenë në gjendje të krijojnë më shumë se një llogari aktive për çdo identitet të verifikuar. Çdo tentativë për hapje të shumëfishtë duhet të sinjalizohet automatikisht në sistemin qendror të monitorimit *online* (SQMO) të administruar nga Autoriteti i Mbikëqyrjes së Lojërave të Fatit (AMLF);

h) Platforma duhet të ruajë dhe të përditësojë automatikisht statusin e identifikimit të përdoruesit ("verifikuar"/"në pritje"/"bllokuar"), duke siguruar që asnjë përdorues i paidentifikuar plotësisht të mos ketë akses në lojëra apo në transaksione.

1.4 Integrimi me sisteme të treta:

a) Sistemi i basteve sportive *online* duhet të jetë ndërtuar në mënyrë që të garantojë **ndërveprueshmëri të sigurt e të qëndrueshme** me sistemet e palëve të treta, të cilat janë të nevojshme për funksionimin ligjor dhe teknik të aktivitetit të lojërave të fatit;

b) Integrimi i sistemit duhet të sigurojë shkëmbimin e plotë, në kohë reale dhe të verifikueshme të të dhënave ndërmjet Autoritetit të Mbikëqyrjes së Lojërave të Fatit (AMLF), për qëllime kontrolli, monitorimi dhe mbikëqyrjeje të aktivitetit të basteve sportive *online*; sistemit qendror të monitorimit *online* (SQMO), për transmetimin automatik të të dhënave mbi bastet e vendosura, fitimet, pagesat, faturat dhe çdo transaksion të regjistruar nga platforma, sipas përcaktimeve ligjore; institucioneve financiare dhe agjentëve të licencuar të pagesave, për kryerjen e transaksioneve financiare vetëm nëpërmjet kanaleve të miratuara dhe të gjurmuara bankare; dhe sistemeve të administratës tatimore dhe doganore, për raportimin automatik të taksave dhe tarifave, sipas dispozitave fiskale në fuqi;

c) Sistemi duhet të lejojë **komunikim të sigurt** dhe **transferim të dhënash të enkriptuara**, duke siguruar mbrojtjen e informacionit financiar e personal të lojtarëve, në përputhje me kërkesat e **ligjit për mbrojtjen e të dhënave personale** dhe **akteve nënligjore të miratuara nga AMLF**-ja;

ç) Platforma duhet të jetë **teknikisht e integruar me SQMO** nëpërmjet një ndërfaqeje të miratuar nga AMLF-ja, e cila garanton:

i. regjistrimin automatik të çdo bilete basti të vendosur *online*;

ii. dërgimin e menjëhershëm të të dhënave mbi pagesat dhe fitimet;

iii. pamundësinë e manipulimit, fshirjes apo ndryshimit të të dhënave pas regjistrimit;

d) Çdo sistem, që nuk përmbush kërkesat e integrimit sipas kësaj nënpike, **nuk mund të konsiderohet funksional e nuk mund të përdoret për ushtrimin e aktivitetit të basteve sportive *online*** në Republikën e Shqipërisë;

dh) Sistemi i basteve sportive *online*, përpara se të fillojë të jetë funksional për lojtarët, duhet të sigurojë shkëmbimin e të dhënave me sistemet e përcaktuara në këtë nënpikë, sisteme këto që nga ana tjetër e tyre duhet të respektojnë parashikimet e kuadrit rregullator në fuqi.

1.5 Mbajtja e regjistrave të ngjarjeve dhe të transaksioneve:

a) Sistemi duhet të mbajë regjistra të detajuar për të gjitha ngjarjet e transaksionet, që ndodhin në platformë;

b) Përdoruesit duhet të kenë role të përcaktuara dhe privilegje të kontrolluara për të aksesuar e për të vepruar;

c) Veprimet e përdoruesve, si: vendosja e basteve, transferimet e fondeve dhe ndryshimet e llogarive duhet të regjistrohen dhe të jenë të lidhura me identifikimin e tyre unik;

ç) Sistemi duhet të ketë të implementuar mekanizma, që mundësojnë ruajtjen e regjistrave në mënyrë të sigurt dhe mbrojtjen nga akseset e paautorizuara;

d) Sistemi duhet të ketë mekanizma për auditimin e monitorimin e regjistrave për të identifikuar dhe ndjekur aktivitetet e paligjshme ose të dyshimta;

dh) Ky auditim duhet të përfshijë shënime të detajuara të veprimeve të përdoruesve dhe të ndërveprimeve me regjistrat;

e) Sistemi duhet të ketë të implementuar mekanizma gjurmimi dhe auditimi për çdo ndryshim që ndodh në sistem dhe për çdo veprim të kryer nga përdoruesit. Gjurmët e veprimeve dhe të auditimit duhet të jenë të pamundura për t'u ndryshuar. Në gjurmët (*logs*) duhet të ruhen minimalisht të dhënat: numri i letërnjoftimit të përdoruesit ose të administratorit, data/ora, IP-ja e

pajisjes, veprimi i kryer dhe statusi i veprimit. *Log*-et mund të arkivohen, por, në asnjë rast, nuk duhet të fshihen;

ë) Çdo incident raportohet brenda 24 (njëzet e katër) orëve pranë autoriteteve mbikëqyrëse;

f) Të dhënat e *log*-eve të rrjetit duhet të ruhen minimalisht për 5 (pesë) vjet, në mënyrë që të jenë të disponueshme për auditim nga AMLF-ja;

g) Monitorimi duhet të jetë aktiv 24/7 dhe të gjenerojë njoftime automatike për anomalitë, ndërprerjet ose aktivitetet e dyshimta.

1.6 Baza e të dhënave:

a) Baza e të dhënave duhet të ketë minimalisht formatin "*Replikim master–slave*" për siguri dhe performancë;

b) Në çdo kohë të aktivitetit të platformës duhet të ketë kopje rezervë automatike dhe politika ruajtjeje. Kopjet rezervë duhet të jenë të enkriptuara dhe të plotësojnë standardin 3-2-1 (një kopje primare dhe dy kopje rezervë. Kopjet rezervë duhet të jenë në dy media/teknologji të ndryshme). Në çdo rast, një nga kopjet e *backup*-it duhet të jetë në distancë minimalisht 50 km nga kopja primare;

c) Baza e të dhënave duhet të mundësojë enkriptim në pushim (*at rest*), minimalisht me AES-256 ose ekuivalent, dhe enkriptim gjatë transmetimit (*in transit*), me minimalisht TLS 1.3 ose ekuivalent;

ç) Baza e të dhënave duhet të ketë të integruar mekanizmat e maskimit të **të dhënave (*data masking*)** për të dhëna personale (p.sh. numra telefoni, dokumente ID);

d) Të paktën një kopje e plotë e përditësuar e të gjithë bazës së të dhënave duhet të ruhet brenda territorit të vendit, ku është licencuar organizatori/subjekti;

dh) Struktura e bazës së të dhënave duhet të mundësojë:

i. historik të plotë të basteve, të fitimeve, të humbjeve, të krediteve, të bonuseve;

ii. auditim të çdo ndryshimi;

iii. integrim me API-të e autoriteteve shtetërore;

e) Baza e të dhënave duhet të ruajë *log*-e të plota të çdo operacioni: *insert*, *update*, *delete*, *select*;

ë) Çdo ndryshim në të dhënat e përdoruesve dhe bastet duhet të ruhet në tabela auditimi të ndara;

f) *Log*-et duhet të përmbajnë minimalisht:

i. ID-në e përdoruesit/operatorit;

ii. kohën (*timestamp UTC);*

iii. IP-në e origjinës;

iv. llojin e operacionit dhe të dhënat e prekura/ndryshuara;

g) *Log*-et duhet të jenë të pandryshueshme (*immutable*). Ato mund të arkivohen, por, në asnjë rast, të fshihen;

gj) Çdo gjurmë (*log*) duhet të ketë një numër identifikues unik;

h) Të paktën një kopje e plotë e përditësuar e të gjithë bazës së të dhënave duhet të ruhet brenda territorit të vendit, ku është licencuar organizatori/subjekti.

1.7 Ndërfaqet *web* dhe aplikacionet *mobile:*

a) Sistemi duhet të ketë një ndërfaqe të disponueshme 24/7, që është e aksesueshme nëpërmjet *web*-it dhe/ose aplikacionit, pavarësisht llojit e tipit të pajisjes që përdoret;

b) Përshtatshmëria e ndërfaqes nuk duhet të jetë e pavarur nga të dhënat e pajisjes, nga e cila ajo po aksesohet, si: sistemi i operimit, rezolucioni, dimensionet e ekranit;

c) Ndërfaqja duhet të lejojë përdoruesit të krijojnë llogari, të kyçen e të menaxhojnë profilin e tyre;

ç) Ndërfaqja dhe/ose aplikacioni duhet të jetë e/i përshtatshme/ëm për t'u aksesuar nga çdo pajisje elektronike;

d) Ndërfaqja dhe/ose aplikacioni duhet të jetë e/i përshtatshme/ëm pavarësisht sistemit operativ të përdorur dhe të ofrojë funksionalitete të njëjta me versionin e faqes së internetit;

dh) Infrastruktura *hardware* duhet të ketë kapacitet të mjaftueshëm për të përballuar ngarkesa të larta të përdoruesve dhe të trafikut, duke garantuar kohë përgjigjeje nën 200 ms për çdo transaksion dhe vazhdimësi të shërbimit *(uptime e" 99.9%)*;

e) Performanca duhet të përfshijë përpunimin në kohë reale të basteve, llogaritjeve të kuotave dhe të transaksioneve;

ë) Sistemi duhet të funksionojë në një infrastrukturë *hardware* të sigurt, të certifikuar dhe të besueshme, që përfshin serverat, pajisjet e rrjetit, pajisjet e ruajtjes së të dhënave dhe komponentët e sigurisë fizike, në përputhje me ligjin nr. 155/2015, "Për lojërat e fatit në Republikën e Shqipërisë", të ndryshuar;

f) Në menunë, ku shfaqet bilanci i kreditit apo i debitit të klientit, duhet të shfaqet gjendja reale e llogarisë së klientit në çdo kohë, sipas monedhës së llogarisë (lek, euro, dollar amerikan), për çdo rast kur klienti është i loguar;

g) Çdo konvertim i mundshëm nga një valutë në një tjetër duhet të paraqitet qartësisht për klientët së bashku me rregullat e konvertimit. Kur konvertimi kryhet në kredite, konvertimi duhet të paraqitet qartësisht për klientin;

gj) Ndërfaqja duhet të paraqesë informacion për klientin për përzgjedhjet që ai ka bërë, llojin e lojës/bastit që ka zgjedhur të luajë, koeficientët e pranuar. Formati i koeficienteve, që do të merren në konsideratë në lojë, si dhe rregullorja e çdo tipologjie loje duhet të jenë qartësisht të përcaktuara në termat e në kushtet, që do të publikohen në ndërfaqen në *web*/*mobile* ose aplikacione;

h) Ndërfaqja *web* ose *mobile* duhet të jetë minimalisht në dy gjuhë (shqip dhe anglisht) me mundësi zgjedhjeje nga përdoruesi;

i) Ndërfaqja *web* ose *mobile* duhet të ketë të përfshira raporte për përdoruesin mbi veprimtarinë e tij të lojës;

j) Ndërfaqja duhet të ketë kohë ngarkimi jo më të lartë se 3 (tri) sekonda për rrjete 4G;

k) Ndërfaqja *web* ose *mobile* duhet të ketë të integruar mekanizmat e skadimit të sesionit pas një periudhe pasiviteti të përdoruesit;

l) Ndërfaqja duhet të ketë të integruara protokollet HTTPS me TLS të versionit të fundit stabël të lëshuar, në çdo pikë fundore (*endpoint*);

ll) Ndërfaqja duhet të administrojë të dhënat personale, në përputhje me legjislacionin shqiptar për mbrojtjen e të dhënave personale dhe GDPR-në;

m) Të gjitha fushat sensitive (llogari, ID, karta) duhet të jenë të maskuara në ndërfaqen e përdoruesit (UI);

n) Ndërfaqja duhet të mundësojë ngarkimin e dokumenteve (ID, pasaportë) në format *.pdf*;

nj) Ndërfaqja duhet të ketë të integruara mekanizma mbrojtës nga sulmet dashakeqe, si: *Anti-CSRF tokens, rate-limiting* për *API, CAPTCHA/reCAPTCHA* për log-in dhe regjistrim;

o) Ndërfaqja duhet të ketë të integruara mekanizmat, që mundësojnë që të gjitha të dhënat sensitive (fjalëkalime, ID, kartat, bilancet, historiku i basteve, të dhënat personale) të ruhen në bazën e të dhënave dhe jo në *browser* apo në pajisjen lokale;

p) Çdo komunikim me bazën e të dhënave dhe sistemin qendror duhet të kryhet në mënyrë të enkriptuar me nivel enkriptimi minimalisht AES256 ose ekuivalent;

q) Ndërfaqja duhet të ketë të publikuara, në një vend të dukshëm për përdoruesin, në një gjuhë të kuptueshme, të gjitha rregullat e lojës, kufizimet e mundshme dhe të gjitha mundësitë e fitimit ose të humbjes së lojtarëve;

r) Të gjitha shumat, që lidhen me lojën dhe fitimet, duhet të kuotohen me simbolin e valutës, me të cilën lojtari është duke luajtur;

rr) Lojërat e hapura me ndërfaqe "*full screen*", gjatë të gjithë kohës, duhet të mundësojnë shfaqjen e orës reale;

s) Lojërat e hapura me ndërfaqe "*full screen*" duhet të kenë në çdo moment një opsion të dukshëm për të dalë nga loja;

sh) Ndërfaqja duhet të përmbajë në mënyrë të dukshme informacion mbi licencën e organizatorit, emrin e organizatorit, sipas licencës që disponon, adresën e organizatorit, kontaktin e organizatorit dhe një njoftim për përgjegjshmërinë në lojë, i cili duhet të informojë përdoruesit për dëmet që mund të shkaktojë pjesëmarrja e pakontrolluar në lojërat e fatit sipas rregullores së publicitetit të miratuar nga Komisioni i Licencave;

t) Kushtet e përdorimit dhe rregulloret, që lidhen me lojën, duhet të jenë në ndërfaqen kryesore ose në një vendndodhje jo më të fshehur sesa vetëm një klikim nga ndërfaqja kryesore;

th) Ndërfaqja duhet të ofrojë në mënyrë të lehtë për lojtarët një mundësi për të vendosur një kufi mbi shumën që mund të depozitohet dhe/ose luhet dhe/ose mbi humbjet që mund të ndodhin, brenda një periudhe të caktuar kohore, gjatë regjistrimit ose menjëherë pas regjistrimit në hyrjen e parë, dhe kjo mundësi mbetet e disponueshme për lojtarin në çdo kohë pas regjistrimit;

u) Ndërfaqja duhet të ofrojë në mënyrë të lehtë për lojtarët mundësinë për t'u përjashtuar vetë, në mënyrë të përcaktuar ose të pacaktuar dhe këto kufizime zbatohen për të gjitha lojërat që ofrohen nga i licencuari në të njëjtën faqe interneti;

v) Në rastet kur ndërfaqja u ofron lojtarëve, që janë vetëpërjashtuar për një periudhë të përcaktuar, mundësinë për të ulur periudhën e përjashtimit ose për ta revokuar atë, ulja ose revokimi mund të ndodhë vetëm pas kalimit të 24 (njëzet e katër) orëve nga momenti kur i licencuari ka marrë një njoftim të tillë;

x) Ndërfaqja duhet t'u ofrojë lojtarëve, që kanë vendosur vetë kufij ose vetëpërjashtime, mundësinë për t'i reduktuar kufijtë, duke i bërë më të rreptë, dhe/ose për të zgjatur periudhën e përjashtimit. Çdo ndryshim i tillë duhet të hyjë në fuqi menjëherë pasi i licencuari të ketë marrë njoftimin përkatës;

xh) Sistemi nuk duhet të pranojë asnjë bast nga një lojtar në kundërshtim me një kufi ose përjashtim të vendosur nga vetë lojtari;

y) Sistemi përjashton nga listat e postimeve "marketing" lojtarët, që kanë zgjedhur vetëpërjashtimin, për aq kohë sa vetëpërjashtimi është në fuqi. Përjashtimi nga lista e postimeve duhet të hyjë në fuqi jo më vonë se 24 (njëzet e katër) orë pas momentit që lojtari zgjedh vetëpërjashtimin;

z) Sistemi duhet të mundësojë, si më poshtë:

i. të jetë në gjendje t'u ofrojë lojtarëve historikun e transaksioneve të lojërave;

ii. të jetë në gjendje t'u ofrojë lojtarëve historikun e transaksioneve financiare, duke përfshirë totalin e depozitave, tërheqjeve, fitimeve/humbjeve dhe pozicionin neto, total;

iii. të ofrojë informacion të detajuar për secilën lojë;

iv. të shfaqë emrin e secilës lojë;

v. të komunikojë kufizimet e lojës;

vi. të ofrojë udhëzime se si luhet;

vii. të ofrojë një tabelë pagesash për të gjitha shpërblimet dhe veçoritë speciale;

viii. të shfaqë bilancin aktual të llogarisë së lojtarit;

ix. të shfaqë në çdo kohë bilancin e llogarisë së lojtarit dhe monedhën përkatëse.

1.8 Infrastruktura mbajtëse:

a) Sistemi duhet të sigurojë funksionim të vazhdueshëm (24/7) dhe rikuperim automatik, në rast dështimi;

b) Komponentët kritikë (serverat, databazat, API) duhet të kenë ***redundance*** të plotë (N+1);

c) Infrastruktura duhet të përballojë dështime të pjesshme pa ndërprerë shërbimin (nuk duhet të ketë *single point of failure*);

ç) *Datacenter*-i, ku është hostuar sistemi, duhet të jetë i certifikuar minimalisht me standardin ISO/IEC 27001 dhe 22301, dhe të ketë akses të kontrolluar fizikisht, nëpërmjet kartave biometrike, CCTV, dhe regjistrim hyrje-daljesh;

d) Të gjithë komponentët e shërbimet duhet të jenë nën **kontroll qendror të administrimit, auditimit e të monitorimit**;

dh) Rrjeti duhet të ndahet në zona funksionale:

i. zona e përdoruesve *(front-end)*;

ii. zona e aplikacionit (*application zone*);

iii. zona e bazës së të dhënave (*data zone*);

iv. zona e administrimit dhe auditimit;

e) Ndërveprimet ndërmjet zonave duhet të kufizohen me rregulla të rrepta dhe të dokumentuara të kontrollit të trafikut;

ë) Çdo kufi rrjeti duhet të mbrohet me *firewall*, me rregulla "*default deny*" dhe leje vetëm për portat dhe protokollet e nevojshme;

f) Trafiku hyrës ndaj shërbimeve kritike (baste, pagesa, identifikim) duhet të shpërndahet në mënyrë të ekuilibruar;

g) Çdo përdorues, aplikacion ose shërbim duhet të ketë vetëm nivelin minimal të aksesit, që i nevojitet për funksion;

gj) Duhet të ekzistojnë mekanizma për zbutje të sulmeve volumetrike dhe ruajtje të disponueshmërisë së platformës;

h) Sistemi duhet të përditësohet rregullisht për të eliminuar dobësitë e njohura (*patch management*);

i) Sistemi duhet të ketë mekanizma *backup* dhe rikuperimi për të minimizuar ndërprerjet e shërbimit dhe për të siguruar që aktiviteti i basteve sportive të vazhdojë pa ndërprerje, edhe në rast të dështimeve të pajisjeve, rrjetit, energjisë elektrike dhe situatave emergjente të tjera. Këto mjete dhe teknologji duhet të mundësojnë që dhe në rastet e ndërprerjes së aktivitetit si pasojë e ngjarjeve të paparashikuara, që bëjnë të pamundur vijimin e aktivitetit, platforma dhe sistemi të rikthehen në një kohë të shpejtë, në mënyrë të sigurt, në gjendjen që ishin përpara ndodhjes së ngjarjes së papritur me të dhëna të plota, duke u siguruar që ato janë të pandryshuara dhe të plota;

j) Kjo përfshin përdorimin e serverave të *backup*-it, sistemeve të *power suply*, të mjeteve të *load balancing* dhe të teknologjive të tjera për të siguruar që sistemi të jetë i përgatitur për situata të paparashikuara;

k) Backup-et duhet të kryhen në mënyrë strikte dhe të ruhen në vende të sigurta, të ndryshme nga vendndodhja primare, ku është hostuar sistemi, për të siguruar rikthimin e të dhënave në rastet e nevojshme;

l) Vendndodhja fizike e *mirror servera*-ve dhe e infrastrukturës duhet të jetë e sigurt e të mbrohet nga rreziqet fizike. Kjo përfshin aksesimin e kontrolluar fizik në *datacenter* dhe në sisteme të sigurisë fizike për të parandaluar hyrjet e paautorizuara dhe vjedhjen e pajisjeve fizike;

ll) Duhet të zbatohen mekanizma për mbrojtjen e të dhënave, duke përfshirë enkriptimin e të dhënave, sigurimin e kopjeve *backup* të të dhënave dhe përdorimin e politikave dhe të standardeve të sigurisë për të mbrojtur integritetin dhe konfidencialitetin e të dhënave;

m) Sistemet e monitorimit, *firewall*-et, antiviruset dhe *software*-t e mbrojtjes së të dhënave duhet të jenë të implementuara për të mbrojtur sistemin nga rreziqet e sigurisë. Të gjitha këto elemente duhet të jenë në përputhje me standardet dhe direktivat e miratuara nga Bashkimi Evropian;

n) Sistemet e ndërprerjes së energjisë (UPS) dhe planifikimi i rezervave të energjisë duhet të jenë të përfshira për të mbajtur sistemin në funksionim, në raste emergjente;

nj) Subjekti duhet të sigurojë zinxhirin e furnizimit të pajisjeve, për të siguruar që dështimi i një pajisjeje ose mosofrimi i mbështetjes teknike nga prodhuesi të mos ndikojë dhe të mos impaktojë në dështimin e sistemit. Asnjë element i infrastrukturës nuk duhet të funksionojë/operojë, nëse ka status *End of Support* ose *End of Life* nga prodhuesit përkatës;

o) Për të minimizuar vonesat dhe dështimet e lidhjes, duhet të ketë minimalisht dy lidhje interneti të dedikuara nga dy burime të ndryshme me kapacitet të lartë, një primar dhe një *backup*;

p) Në rrjet duhet të jenë implementuar mekanizma, në mënyrë që rrjeti të jetë i mbrojtur nga rreziqet e sigurisë dhe të ketë mekanizma të sigurisë për të parandaluar akseset e paautorizuara dhe sulmet nga të tretët;

q) Sistemet e ndërprerjes së energjisë (UPS) dhe planifikimi i rezervave të energjisë duhet të jenë të përfshira për të siguruar që rrjeti të vazhdojë të funksionojë edhe në raste humbjeje të energjisë;

r) Regjistrat elektronikë duhet të jenë të strukturuar në mënyrë kronologjike dhe të pandryshueshme, duke përmbajtur të dhëna të detajuara për çdo ngjarje, si: data, ora, përdoruesi, IP adresa dhe rezultati i veprimit. Ruhen për jo më pak se 5 (pesë) vjet.

rr) Regjistrat duhet të mbrohen nga modifikimi, fshirja apo manipulimi i paautorizuar, duke përdorur mekanizma kriptografikë të integritetit të të dhënave (*hashing* dhe *timestamping*).

1.9 Rrjeti në sistemet e basteve *online:*

a) Rrjeti duhet të jetë i dedikuar, me kapacitet të lartë (minimumi 1 Gbps) dhe me *redundance* të plotë për të përballuar trafikun intensiv të basteve *online*;

b) Për të garantuar cilësi dhe qëndrueshmëri, rrjeti duhet të ketë dy lidhje të pavarura interneti (dual ISP) dhe sistem *failover* automatik;

c) Rrjeti duhet të ketë kanal rezervë komunikimi (*redundant path*) për të shmangur ndërprerjet e shërbimit;

ç) Të gjithë komponentët e rrjetit duhet të jenë të mbrojtur nga akseset e paautorizuara, DDoS, *spoofing* dhe *intrusion attempts* nëpërmjet *firewall*-eve, VPN-ve dhe IDS/IPS-ve të avancuara;

d) Të gjitha komunikimet e brendshme dhe të jashtme duhet të jenë të enkriptuara me SSL/TLS 1.3 ose protokolle ekuivalente të sigurisë;

dh) Subjekti duhet të dokumentojë teknologjitë e rrjetit, konfigurimet, testimet dhe auditimet periodike, për të verifikuar përputhjen me standardet e kërkesat ligjore.

1.10 Dokumentimi:

a) Platforma duhet të jetë e dokumentuar mirë për të lehtësuar përdorimin, mirëmbajtjen e zhvillimin e mëtejshëm;

b) Manuali i përdoruesit, dokumentacioni teknik dhe udhëzimet e instalimit e të konfigurimit duhet të jenë të disponueshme, të përditësohen rregullisht dhe të verifikohen nga AMLF-ja në terren;

c) Organizatori duhet të mbajë dokumentacion të përditësuar lidhur me elementet kryesore të ekosistemit të platformës së tij, të cilin duhet t'ia vendosë në dispozicion dhe AMLF-ja. Ky dokumentacion duhet të përfshijë minimalisht elementet, si më poshtë vijon:

i. pajisjet *hardware* të përdorura, përfshirë markën, modelin dhe çdo element tjetër, që identifikon pajisjen. Gjithashtu, duhet të specifikohet dhe vendndodhja fizike e pajisjes. Kjo vendndodhje duhet të deklarohet edhe në rast se organizatori përdor infrastrukturë "*on cloud*";

ii. të gjitha makinat virtuale të përdorura (nëse ka të tilla), përfshirë elemente që identifikojnë makinën virtuale dhe vendndodhjen, ku ato janë të hostuara;

iii. lidhjet ndërmjet nyjave të rrjetit;

iv. aplikacionet e instaluara në *hardware* dhe/ose makinat virtuale duke përfshirë dhe një përshkrim të specifikimeve të tyre teknike;

ç) Organizatori duhet të marrë më parë miratimin paraprak nga AMLF-ja për çdo ndryshim të sistemit dhe të rregulloreve, përpara se ky ndryshim të fillojë të aplikohet nga organizatorë.

III. FATURAT DHE TRANSAKSIONET E PAGESAVE

1. Platforma duhet të ofrojë një gamë të sigurt të opsioneve të pagesës për përdoruesit. Kjo përfshin përdorimin e protokolleve të sigurisë për transmetimin e të dhënave të pagesave dhe përdorimin e metodave të sigurta të pagesave, që lejon legjislacioni bankar.

2. Kërkesat e sigurisë, si protokollet e enkriptimit dhe verifikimi i transaksioneve, duhet të jenë të implementuara për të mbrojtur të dhënat financiare të përdoruesve.

3. Platforma duhet të zbatojë masat e nevojshme për të mbrojtur financat e përdoruesve nga mashtrimi dhe aksesi i paautorizuar, në përputhje me direktivat dhe legjislacionin shqiptar dhe të Bashkimit Evropian.

4. Platforma duhet të jenë transparente lidhur me politikat e pagesave, tarifat dhe komisionet e aplikueshme për përdoruesit.

5. Platforma, gjithashtu, duhet të jetë e pajtueshme me rregulloret dhe legjislacionin e aplikueshëm lidhur me financat, duke përfshirë identifikimin e përdoruesve, raportimin e transaksioneve dhe zbatimin e masave kundër pastrimit të parave.

6. Software-i duhet të jetë i aftë për të mbështetur një gamë të gjerë, të verifikuar dhe të miratuar nga AMLF-ja, të llojeve të bastit, të disponueshme në sporte të ndryshme, në përputhje me ligjin nr.155/2015, "Për lojërat e fatit në Republikën e Shqipërisë", të ndryshuar. Kjo përfshin bastet e thjeshta (p.sh. rezultatin përfundimtar), bastet e kombinuara (kombinimi i disa ngjarjeve të ndryshme në një kupon të vetëm), bastet *live* në kohë reale, si dhe bastet e parashikimeve të veçanta (p.sh. numri i golave, kartonëve etj.), gjithmonë brenda kufijve të përcaktuar nga licenca dhe rregullorja përkatëse.

7. Çdo lloj basti që ofrohet duhet të jetë i dokumentuar dhe i miratuar nga AMLF-ja përpara vënies në dispozicion të lojtarëve.

8. Protokollet e pagesave, që do të mundësojë platforma, duhet të integrohen në SQMO.

9. Çdo **biletë basti *online*** dhe **faturë elektronike** duhet të përmbajnë të paktën elementet e mëposhtme ligjore dhe teknike:

a) Numrin unik të identifikimit të biletës dhe të faturës;

b) Datën dhe orën e vendosjes së bastit;

c) Emrin tregtar dhe NIPT-in e operatorit të licencuar;

ç) Identifikuesin unik të lojtarit (ID ose *username*);

d) Përshkrimin e ngjarjes sportive, koeficientin (*odd*) dhe shumën e bastit;

dh) Shumën totale të fitimit potencial;

e) Referencën e sistemit të pagesës (metoda e përdorur – bankë, kartë, portofol elektronik, agjenci pagesash);

ë) Vërtetimin automatik të sistemit (nënshkrim elektronik ose kod sigurie);

f) Numrin e licencës së operatorit dhe logon e institucionit mbikëqyrës;

g) Njoftimin ligjor për përgjegjësinë e lojtarit dhe ndalimin për të miturit, sipas programit të mbrojtjes së lojtarit dhe të rregullores së publicitetit ("Lojërat e fatit krijojnë varësi. Kujdes në ushtrimin e tyre të tejzgjatur!).

IV. PARIMET E SIGURISË DHE KUSHTET E KONTROLLIT

1. Integriteti dhe transparenca e të dhënave

1.1 Të gjitha veprimet e sistemit (bastet, fitoret, humbjet, anulimet, gabimet, depozitimet dhe tërheqjet) duhet të regjistrohen **në kohë reale** dhe në **format të pandryshueshëm**, të cilat mund të rikrijohen nga regjistrat teknikë (*logs*).

1.2 Çdo ndryshim në të dhëna duhet të ruajë historikun origjinal dhe të jetë i gjurmueshëm për auditim e verifikim.

2. Masat teknike të sigurisë

2.1 Përdorimi i certifikatave SSL për mbrojtjen e të dhënave në transmetim;

2.2 Zbatimi i standardeve ndërkombëtare: **ISO 9001, ISO/IEC 27001, ISO/IEC 27017** dhe **ISO/IEC 27018** për menaxhimin e sigurisë dhe mbrojtjen e të dhënave personale;

2.3 Enkriptimi i të dhënave, autentifikimi shumëfaktorësh, autorizimi dhe kontrollet e qasjes për të garantuar, që vetëm personat e autorizuar kanë akses.

3. Mbrojtja fizike dhe logjike e infrastrukturës

3.1 Serverat, rrjetet dhe pajisjet duhet të jenë të mbrojtura fizikisht dhe logjikisht dhe të survejuara për 24 (njëzet e katër) orë;

3.2 Të sigurohet *backup* ditor dhe plan rikuperimi nga fatkeqësitë (*disaster recovery plan*);

3.3 Të dhënat personale dhe financiare ruhen sipas praktikave më të mira të industrisë dhe standardeve ISO/IEC.

4. Monitorimi dhe auditimi i sigurisë

4.1 Sistemet duhet të monitorohen vazhdimisht për incidente dhe anomalitë e sigurisë;

4.2 Auditime të pavarura të sigurisë kryhen periodikisht dhe raportohen pranë Autoritetit të Mbikëqyrjes së Lojërave të Fatit;

4.3 Subjekti i licencuar duhet të hartojë, të zbatojë dhe të mirëmbajë një plan të sigurisë së informacionit (PSI), i cili përmban:

i. analizën e risqeve;

ii. politikat e sigurisë;

iii. masat parandaluese dhe korrigjuese;

iv. procedurat e reagimit ndaj incidenteve.

4.4 Ky plan duhet të përditësohet të paktën një herë në vit dhe të dërgohet për miratim pranë Autoritetit të Mbikëqyrjes së Lojërave të Fatit (AMLF).

5. Politikat dhe menaxhimi i incidenteve

5.1 Subjektet zbatojnë **politikë të integruar të sigurisë së informacionit**, duke përfshirë menaxhimin e rrezikut, planin e reagimit ndaj incidenteve dhe planin e rikuperimit pas fatkeqësive;

5.2 Çdo incident që prek sistemin raportohet menjëherë tek Autoriteti i Mbikëqyrjes së Lojërave të Fatit.

6. Dokumentimi teknik e procedural

6.1 Subjekti dokumenton të gjitha masat e zbatimit të sigurisë dhe të auditimeve teknike, përfshirë regjistrat e *log*-eve, planet e rikuperimit dhe raportet e auditimit;

6.2 Dokumentacioni mbahet i azhurnuar dhe është i gatshëm për shqyrtim nga autoritetet mbikëqyrëse.

V. CERTIFIKIMI I SISTEMIT

1. Organizatori i lojës ose subjekti që zhvillon e mirëmban platformën e basteve *online* duhet të disponojë certifikimet e mëposhtme, për sa kohë që ato lëshohen nga autoritete të akredituara, sipas legjislacionit shqiptar dhe/ose evropian:

i. ISO/IEC 27001:2022 – Menaxhimi i Sigurisë së Informacionit;

ii. ISO/IEC 22301 – Menaxhimi i Vazhdimësisë së Biznesit;

iii. ISO/IEC 20000 – Menaxhimi i Shërbimeve IT;

iv. PCI DSS – Siguria e të Dhënave të Kartave të Pagesës;

v. ISO 9001 **Sistemet e Menaxhimit të Cilësisë;**

vi. GLI-19 (*Gaming Laboratories International*) standard teknik për sistemet e lojërave të fatit *online*;

vii. GLI – 33 (*Gaming Laboratories International*) standard teknik për sistemet e lojërave të fatit *online*).

2. Certifikimet duhet të jenë të vlefshme dhe aktive gjatë gjithë kohës së ushtrimit të veprimtarisë dhe operatori është i detyruar të depozitojë pranë AMLF-së kopjet e certifikatave për verifikim dhe auditim.

3. Certifikimi përfshin verifikimin e funksionalitetit, të sigurisë, të integritetit të të dhënave, auditueshmërisë dhe të disponueshmërisë së sistemit.

VI. DISPOZITA TË FUNDIT

Ngarkohen Autoriteti i Mbikëqyrjes së Lojërave të Fatit, Komisioni i Licencave dhe subjektet e licencuara të lojërave të fatit në kategorinë "Baste sportive *online*" për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi 30 ditë pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama