Udkast til forskrift

Spilsystemers pålidelighed og informationssikkerhed i henhold til spilleloven

Indhold

Spilsystemers pålidelighed og informationssikkerhed i henhold til spilleloven....1
1 Retsgrundlag, anvendelsesområde og definitioner....2
1.1 Tilsynsmyndighedens beføjelse til at udstede påbud....2
1.2 Lovgivning....2
1.3 Anvendelsesområde....2
1.4 Definitioner....2
2 Akkreditering af et kontrolorgan....3
3 Generel informationssikkerhedspraksis....3
4 Kontrolorgan, der udfører informationssikkerhedstests....3
4.1 Kompetenceområde....4
5 Fornyelse af informationssikkerhedstestning....4
6 Informationssikkerhedstestning med negativt resultat....5
7 Sårbarhedsscanning....5
8 Sårbarhedsscanninger udført i forbindelse med informationssikkerhedstestning....6
9 Udbedring af sårbarheder....6
10 Brug af udstedte certifikater....6
11 Undtagelser....7
12 Ikrafttrædelse....7

1 Retsgrundlag, anvendelsesområde og definitioner

1.1 Tilsynsmyndighedens beføjelse til at udstede påbud

Tilsynsmyndighedens beføjelse til at udstede bindende påbud er baseret på spillelovens (xx/2025) § 44, stk. 6. I henhold til nævnte stykke kan tilsynsmyndigheden udstede mere detaljerede bestemmelser om pålideligheden af spilsystemer, lotteriudstyr og lotterimetoder, der anvendes til drift af spil, om tekniske krav til sikring af, at lodtrækningen er vilkårlig, om den mere detaljerede form og indholdet af kontrolorganets undersøgelse og godkendelse og om de betingelser, som kontrolorganet skal opfylde for at blive godkendt af myndigheden.

I henhold til spillelovens § 57 er tilsynsmyndigheden det finske tilsynsorgan. I henhold til lovens § 106 fungerer den nationale politistyrelse som den kompetente myndighed, der er nævnt i § 57, indtil den 31. december 2026.

1.2 Lovgivning

Følgende lovgivning er relevante for genstanden af denne forskrift:

- spilleloven (xx/2025)
- lov om administrative procedurer (434/2003)
- lov om databeskyttelse (1050/2018)
- EU's generelle forordning om databeskyttelse (2016/679).

1.3 Anvendelsesområde

Denne lovgivning finder anvendelse på en juridisk eller fysisk person som nævnt i spillelovens kapitel 1, § 2, stk. 1, til hvem der er tildelt en eksklusiv licens eller licens til spilleaktiviteter i henhold til spilleloven.

Den eksklusive licens er omfattet af § 5 i spilleloven, og spillelicensen er omfattet af § 6.

1.4 Definitioner

For så vidt angår denne lovgivning, gælder følgende definitioner: I denne forskrift betyder:

- *eksklusiv licens*: en licens, der er udstedt for de typer spil, der er nævnt i spillelovens § 5
- *spillelicens:* en licens, der er udstedt til de typer spil, der er nævnt i spillelovens § 6

- *spiltransaktion:* den indsats, som spilleren har gjort i spillet, den udfaldsmulighed, som spilleren har valgt, de valg, som spilleren har truffet, og som er relevante for spillets udfald og resultaterne af markederne og udtrækningerne, samt eventuelle gevinster og tab, der er registreret i spilsystemet hos indehaveren af en eksklusiv licens eller spillicens.
- *spillerkontotransaktion:* kontoposteringer.
- *spilsystem:* et onlineinformationssystem, der anvendes af eller på vegne af spiloperatøren til drift af spil.

2 Akkreditering af et kontrolorgan

Licensindehaveren er ansvarlig for pålideligheden af sit lotteriudstyr og sine spilsystemer samt for at udføre de revisioner, der foretages for at sikre denne pålidelighed. Vurderingen af pålidelighed og sikkerhed foretages af et eksternt akkrediteret kontrolorgan. Kontrolorganet skal være akkrediteret i overensstemmelse med Europa-Parlamentets og Rådets forordning (EF) nr. 765/2008 om kravene til akkreditering og markedsovervågning i forbindelse med markedsføring af produkter og om ophævelse af forordning (EØF) nr. 339/93.

Akkreditering kan gives til kontrolorganer af det nationale akkrediteringsorgan FINAS (den finske akkrediteringstjeneste). Et udenlandsk akkrediteringsorgan kan også fungere som akkrediteringsorgan, hvis det er medlem af den europæiske akkrediteringsorganisations multilaterale anerkendelsesordning (EA MLA) inden for det relevante kompetenceområde. Licensindehaveren er forpligtet til at sikre, at den eksterne operatør, der udfører revisionen, har en gyldig akkreditering.

3 Generel informationssikkerhedspraksis

Licensindehaveren er ansvarlig for informationssikkerhed, databeskyttelse og andre tekniske pålidelighedsfunktioner i sine egne spilsystemer. Licensindehaveren skal følge god praksis for informationssikkerhed i forbindelse med sine aktiviteter og bestræbe sig på at minimere trusler mod informationssikkerheden, databrud og andre problemer, der kan bringe spillesystemernes pålidelighed i fare. Licensindehaveren er også forpligtet til at holde øje med ovennævnte faktorer generelt og ikke kun under de regelmæssige inspektioner, der er omhandlet i denne forskrift, for at sikre pålideligheden af sine systemer.

4 Kontrolorgan, der udfører informationssikkerhedstests

Licensindehaveren er forpligtet til at gennemføre sikkerhedstest af sine spilsystemer hvert andet år. Resultatet af informationssikkerhedstestene skal forelægges tilsynsmyndigheden. Informationssikkerhedstests og resultaterne heraf må ikke være mere end to år gamle.

Informationssikkerhedstests skal udføres af et eksternt kontrolorgan, der er akkrediteret i overensstemmelse med ISO/IEC 17025, ISO/IEC 17065 eller ISO/IEC 17020, som angivet i § 2 i denne forskrift. Ved informationssikkerhedstests skal der lægges særlig vægt på beskyttelsen og integriteten af komponenterne i spilsystemer med tilfældige udfald, beskyttelsen af komponenter, der indeholder personoplysninger, og beskyttelsen af betalingsrelaterede komponenter.

Det kontrolorgan, der er ansvarligt for at gennemføre informationssikkerhedstests, og dets personale skal være kompetent og egnet til at gennemføre testene. Den nødvendige kompetence til at udføre informationssikkerhedstests kan blandt andet påvises ved tidligere erhvervserfaring inden for informationssikkerhedstestning, uddannelse eller generelt anerkendte branchecertifikater. Licensindehaveren er forpligtet til at sikre, at de personer, der udfører testningen, er kvalificerede til at udføre informationssikkerhedstestning og efter anmodning kan dokumentere deres kvalifikationer.

Der skal udpeges en person, der skal stå for gennemførelsen af sikkerhedstestning, og som skal være ansvarlig for, at denne gennemføres på passende vis. Den endelige rapport om informationssikkerhedstests skal underskrives og godkendes af den udpegede person og indsendes til tilsynsmyndigheden.

I forbindelse med informationssikkerhedstests skal følgende komponenter samt relaterede sårbarheder eller hændelser som minimum testes:

- mulighed for manipulation af de tilfældige komponenter
- adgang til kundedatabasen
- evne til at påvirke resultatet af spil
- mulighed for at påvirke betalingssystemer eller betalingstransaktioner
- uautoriseret adgang til servere, der bruges til at gemme spil- og spillerkontotransaktioner
- mulighed for at redigere arkiverede data om spilbegivenheder eller spilkontobegivenheder
- ændring eller destruktion af logfiler vedrørende spilsystemer.

4.1 Kompetenceområde

Det akkrediterede kontrolorgan, der udfører revisionen, skal have et kompetenceområde for spil i sin ISO/IEC-akkreditering. Kompetenceområdet skal omfatte de krav, der er fastsat i den finske spillovgivning og tilsynsmyndighedens tekniske forskrifter.

Tilsynsmyndigheden kan indtil den 1. januar 2027 acceptere en akkreditering, der omfatter et kompetenceområde, som vurderes og tildeles på grundlag af tekniske forskrifter udstedt for de danske eller svenske spillesystemer.

5 Fornyelse af informationssikkerhedstestning

Licensindehaveren skal forelægge resultaterne af den godkendte informationssikkerhedstestning for tilsynsmyndigheden. Licensindehaveren må ikke påbegynde driften af hasardspil, før vedkommende har bestået sikkerhedstestningen. Resultatet af informationssikkerhedstestning må ikke være mere end to år gammelt.

Tilsynsmyndigheden kan efter eget skøn give yderligere tid til gennemførelse af sikkerhedstestning, hvorunder driften af spil kan fortsætte.

6 Informationssikkerhedstestning med negativt resultat

Det kontrolorgan, der udfører informationssikkerhedstesten, bør vurdere de sårbarheder, der er konstateret under informationssikkerhedstesten, og deres betydning for spillesystemets pålidelighed. De sårbarheder, der konstateres under vurderingen, bør vurderes ved hjælp af CVSS v3-beregneren (Common Vulnerability Scoring System Calculator version 3), der stilles til rådighed af det nationale teknologiske institut (NIST). For CVSS v3-beregneren vurderes sårbarhedens alvor ud fra basisscoreparametre. Hvis der under sikkerhedstestningen opdages sårbarheder med en beregnet CVSS-værdi på over 5,0, kan testen ikke betragtes som godkendt.

Hvis licensindehaverens informationssikkerhedstestning ikke ender med et godkendt resultat, skal licensindehaveren straks træffe foranstaltninger til at afhjælpe de identificerede informationssikkerhedssårbarheder. Licensindehaveren skal indberette informationssikkerhedstesten med negativt resultat til tilsynsmyndigheden.

Licensindehaveren skal gennemføre en ny sikkerhedstest senest 90 dage efter informationssikkerhedstesten med negativt resultat. Der behøver ikke at blive foretaget en ny informationssikkerhedstestning af hele spilsystemet – i stedet kan informationssikkerhedstestningen målrettes mod de mangler, der førte til den manglende godkendelse. I forbindelse med den fornyede informationssikkerhedstestning skal kontrolorganet sikre, at de sårbarheder, der tidligere er identificeret som begrundelse for manglende godkendelse, er blevet korrigeret.

Implementeringen af hasardspil må ikke påbegyndes, før der er gennemført godkendte og gyldige sikkerhedstests.

7 Sårbarhedsscanning

Ud over sikkerhedstestning er licensindehaverne forpligtet til at overvåge sikkerheden i deres egne systemer ved hjælp af regelmæssige sårbarhedsscanninger. Formålet med sårbarhedsscanninger er at sikre, at de spilsystemer, der anvendes af licensindehaveren, ikke har nogen ydre sikkerhedsmæssige sårbarheder, der kan udnyttes til at angribe spilsystemerne.

Licensindehaveren er forpligtet til at gennemføre en ekstern sårbarhedsscanning en gang om året og rapportere resultaterne til tilsynsmyndigheden. Sårbarhedsscanning kan udføres af et eksternt kontrolorgan, der er akkrediteret i overensstemmelse med ISO/IEC 17025, ISO/IEC 17065 eller ISO/IEC 17020, som angivet i § 2 i denne forskrift.

Licensindehaveren er forpligtet til at afhjælpe sårbarheder, der opdages under sårbarhedsscanning, med opdateringer eller andre hastende afbødende foranstaltninger, hvis korrigerende opdateringer ikke er tilgængelige. Den vurderingsmetode, der er beskrevet i § 6, skal anvendes på sikkerhedsmæssige sårbarheder, der opdages i forbindelse med sårbarhedsscanninger. Hvis den beregnede CVSS-værdi for den identificerede eksterne sårbarhed overstiger 5,0, skal licensindehaveren straks træffe foranstaltninger for at afhjælpe sårbarhederne.

Det kontrolorgan, der er ansvarligt for at gennemføre sårbarhedsscanningen, og dets personale skal være kompetent og egnet til at gennemføre testene. Den nødvendige kompetence til at udføre sårbarhedsscanninger kan bl.a. påvises ved tidligere erhvervserfaring inden for informationssikkerhedstestning, erfaring med anvendelse af sårbarhedsscannere, uddannelse eller almindeligt anerkendte branchecertifikater. Licensindehaveren er forpligtet til at sikre, at de personer, der udfører testningen, er kvalificerede til at udføre sårbarhedsscanninger og på anmodning kan dokumentere deres kvalifikationer.

Der skal udpeges en person, der er ansvarlig for at udføre sårbarhedsscanningen, for at sikre, at den udføres korrekt. Den endelige rapport for sårbarhedsscanningen skal underskrives og valideres af den ansvarlige person og indsendes til tilsynsmyndigheden.

8 Sårbarhedsscanninger udført i forbindelse med informationssikkerhedstestning

Licensindehaveren kan foretage sårbarhedsscanninger som led i informationssikkerhedstestning. De samme krav gælder for sårbarhedsscanninger, der udføres som led i informationssikkerhedstestning, som for andre sårbarhedsscanninger.

9 Udbedring af sårbarheder

Licensindehaveren er forpligtet til regelmæssigt at overvåge informationssikkerheden i sine egne spilsystemer generelt og ikke kun under informationssikkerhedstestning samt til at udbedre sårbarheder, der kompromitterer pålideligheden, når rettelser eller andre udbedrende metoder bliver tilgængelige.

Hvis det ikke er muligt straks at udbedre sårbarhederne, skal licensindehaveren bestræbe sig på at anvende tilgængelige midler til at bekæmpe sårbarhederne og minimere deres konsekvenser.

Hvis CVSS v3-basisscoreværdien for den opdagede eksterne sårbarhed er mindre end 5,0, kan licensindehaveren vurdere, hvor presserende behovet for rettelser er, og efter eget skøn implementere disse rettelser.

10 Brug af udstedte certifikater

Et akkrediteret kontrolorgan, der er godkendt af den tilsynsmyndighed, der er ansvarlig for at gennemføre informationssikkerhedstestning eller sårbarhedsscanning, kan som led i sin kontrol anvende certifikater eller andre attester, der er udstedt til indehaveren af spilsoftwarelicensen. Hvis kontrolorganet anvender eksisterende certifikater som led i kontrollen, skal det vurdere, om certifikaterne kan betragtes som tilstrækkeligt pålidelige beviser for pålideligheden af og informationssikkerheden i spillesystemet tilhørende indehaveren af spilsoftwarelicensen.

11 Undtagelser

Licensindehaveren er forpligtet til straks at indberette eventuelle brud på informationssikkerheden eller databeskyttelsen, som denne opdager, til tilsynsmyndigheden, hvis der er grund til at formode, at pålideligheden af de spilsystemer eller lotteriudstyr, som licensindehaveren anvender, er blevet bragt i fare.

Der stilles ikke krav om, at licensindehaveren skal rapportere mindre sikkerheds- eller databeskyttelseshændelser til tilsynsmyndigheden for spil, hvis hændelsens anslåede effektivitet er af begrænset karakter, eller hvor hændelsen ikke vurderes at have væsentlig indvirkning på spilsystemernes pålidelighed.

12 Ikrafttrædelse

Denne forskrift træder i kraft den X. [måned] 2026.

Den nationale politistyrelse
Spiladministration
Konepajankatu 2, PL 50, 11101 Riihimäki
Telefon +358 295 480 181, poliisi.fi