Projekt rozporządzenia

Niezawodność i bezpieczeństwo informacji systemów gier hazardowych zgodnie z ustawą o grach hazardowych

Spis treści

1 Ramy prawne, zakres i definicje

1.1 Uprawnienie organu nadzorczego do wydawania nakazów

Uprawnienie organu nadzorczego do wydania wiążącego nakazu opiera się na art. 44 ust. 6 ustawy o grach hazardowych (xx/2025). Zgodnie z tym podpunktem organ nadzorczy może wydać bardziej szczegółowe przepisy dotyczące niezawodności systemów gier hazardowych, sprzętu loteryjnego i metod loteryjnych stosowanych w prowadzeniu gier hazardowych, wymagań technicznych zapewniających losowość losowania, bardziej szczegółowej formy i treści dochodzenia i zatwierdzenia przez organ kontrolny oraz warunków, które organ kontrolny musi spełnić, aby uzyskać zatwierdzenie przez organ nadzorczy.

Zgodnie z art. 57 ustawy o grach hazardowych, organem nadzorczym jest Fiński Urząd Nadzoru. Zgodnie z art. 106 ustawy Krajowa Rada Policji pełni funkcję właściwego organu, o którym mowa w art. 57, do dnia 31 grudnia 2026 r.

1.2 Przepisy prawa

Do przedmiotu niniejszego nakazu mają zastosowanie następujące przepisy:

- Ustawa o grach hazardowych (xx/2025)
- ustawa o postępowaniu administracyjnym (434/2003)
- Ustawa o ochronie danych (1050/2018)
- Ogólne rozporządzenie UE o ochronie danych (2016/679)

1.3 Zakres

Przepis ten ma zastosowanie do osoby prawnej lub fizycznej, o której mowa w rozdziale 1, art. 2 ust. 1 ustawy o grach hazardowych, a której na mocy ustawy o grach hazardowych udzielono wyłącznej koncesji lub koncesji na prowadzenie działalności w zakresie gier hazardowych.

Wyłączną koncesję reguluje art. 5 ustawy o grach hazardowych, a koncesję na gry hazardowe - art. 6.

1.4 Definicje

Na potrzeby niniejszego przepisu stosuje się następujące definicje. Do celów niniejszego rozporządzenia:

- *koncesja wyłączna* oznacza koncesję udzieloną na formy gier hazardowych, o których mowa w art. 5 ustawy o grach hazardowych
- *koncesja na prowadzenie gier hazardowych* oznacza koncesję wydaną na gry hazardowe, o których mowa w art. 6 ustawy o grach hazardowych

- *Transakcja hazardowa* oznacza stawkę postawioną przez gracza w grze, opcję wyniku wybraną przez gracza, wybory dokonane przez gracza, które mają znaczenie dla wyniku gry, oraz wyniki rynków i losowań, a także wszelkie wygrane i przegrane zarejestrowane w systemie hazardowym posiadacza wyłącznej koncesji lub koncesji hazardowej
- *transakcja na koncie gracza* oznacza zapisy na koncie.
- *system hazardowy* oznacza internetowy system informacyjny wykorzystywany przez operatora gier hazardowych lub w jego imieniu do prowadzenia działalności hazardowej

2 Akredytacja organu kontrolnego

Posiadacz koncesji jest odpowiedzialny za niezawodność swoich urządzeń loteryjnych i systemów gier hazardowych, a także za przeprowadzanie audytów mających na celu zapewnienie tej niezawodności. Ocena niezawodności i bezpieczeństwa jest przeprowadzana przez zewnętrzną akredytowaną jednostkę kontrolną. Organ inspekcyjny musi posiadać akredytację w rozumieniu rozporządzenia (WE) nr 765/2008 Parlamentu Europejskiego i Rady ustanawiającego wymagania dotyczące akredytacji i nadzoru rynku w związku z wprowadzaniem produktów do obrotu oraz uchylającego rozporządzenie (EWG) nr 339/93.

Akredytacji jednostek kontrolujących może udzielić krajowa jednostka akredytująca FINAS (fińska służba akredytacyjna). Zagraniczna jednostka akredytująca może również pełnić funkcję jednostki akredytującej, jeżeli jest członkiem wielostronnej umowy o wzajemnym uznawaniu (EA MLA) Europejskiej Organizacji Akredytacyjnej w odpowiedniej dziedzinie kompetencji. Posiadacz koncesji jest zobowiązany do zapewnienia, że zewnętrzny operator przeprowadzający audyt posiada ważną akredytację.

3 Ogólne praktyki w zakresie bezpieczeństwa informacji

Posiadacz koncesji jest odpowiedzialny za bezpieczeństwo informacji, ochronę danych i inne techniczne aspekty niezawodności własnych systemów gier hazardowych. Musi on przestrzegać dobrych praktyk w zakresie bezpieczeństwa informacji w swojej działalności i dążyć do zminimalizowania zagrożeń dla bezpieczeństwa informacji, naruszeń ochrony danych i innych problemów, które mogą zagrozić niezawodności systemów gier hazardowych. Jest również zobowiązany do monitorowania wyżej wymienionych czynników poza regularnymi inspekcjami, o których mowa w niniejszym rozporządzeniu, w celu zapewnienia niezawodności swoich systemów.

4 Jednostka kontrolująca przeprowadzająca badanie bezpieczeństwa informacji

Posiadacz koncesji jest zobowiązany do przeprowadzania co dwa lata testów bezpieczeństwa swoich systemów gier hazardowych. Wyniki testów bezpieczeństwa

informacji przedkłada się organowi nadzorczemu. Testy bezpieczeństwa informacji i ich wyniki nie mogą być starsze niż dwa lata.

Badanie bezpieczeństwa informacji przeprowadza zewnętrzny organ kontrolny akredytowany zgodnie z normami ISO/IEC 17025, ISO/IEC 17065 lub ISO/IEC 17020, jak określono w sekcji 2 niniejszego rozporządzenia. Testy bezpieczeństwa informacji powinny zwracać szczególną uwagę na ochronę i integralność elementów systemu gier losowych, ochronę elementów zawierających dane osobowe oraz ochronę elementów związanych z płatnościami.

Organ kontrolny odpowiedzialny za przeprowadzanie testów bezpieczeństwa informacji oraz jego personel muszą posiadać kompetencje i kwalifikacje niezbędne do przeprowadzania takich testów. Niezbędne kompetencje do przeprowadzania testów bezpieczeństwa informacji można wykazać między innymi poprzez wcześniejsze doświadczenie zawodowe w zakresie testowania bezpieczeństwa informacji, szkolenia lub powszechnie uznawane certyfikaty branżowe. Posiadacz koncesji jest zobowiązany do zapewnienia, że osoby przeprowadzające testy posiadają kwalifikacje do przeprowadzania tych testów bezpieczeństwa informacji oraz, na żądanie, do wykazania swoich kwalifikacji.

W celu przeprowadzenia testów bezpieczeństwa należy wyznaczyć osobę odpowiedzialną za ich prawidłowe wykonanie. Ostateczna wersja sprawozdania z badania bezpieczeństwa informacji jest podpisywana i zatwierdzana przez wyznaczoną osobę i przedkładana organowi nadzorczemu.

W kontekście testowania bezpieczeństwa informacji należy przetestować co najmniej następujące elementy, a także powiązane z nimi luki w zabezpieczeniach lub incydenty:

- Możliwość manipulowania elementami losowymi
- Dostęp do bazy danych klientów
- Możliwość wpływania na wynik gier
- Możliwość wpływania na systemy płatności lub transakcje płatnicze
- Nieuprawniony dostęp do serwerów wykorzystywanych do przechowywania transakcji związanych z grami hazardowymi i transakcji na kontach graczy
- Możliwość edycji zarchiwizowanych danych dotyczących wydarzenia hazardowego lub konta hazardowego
- Zmiana lub zniszczenie rejestrów dotyczących systemów gier hazardowych

4.1 Zakres kompetencji

Akredytowany organ inspekcyjny przeprowadzający audyt musi posiadać w ramach swojej akredytacji ISO/IEC zakres kompetencji obejmujący gry hazardowe. Zakres

kompetencji musi obejmować wymagania określone w fińskim ustawodawstwie dotyczącym gier hazardowych oraz przepisy techniczne organu nadzorczego.

Do dnia 1 stycznia 2027 r. organ nadzorczy może akceptować akredytacje, która obejmują zakres kompetencji ocenionych i przyznanych na podstawie przepisów technicznych wydanych dla duńskich lub szwedzkich systemów gier hazardowych.

5 Odnowienie testów bezpieczeństwa informacji

Posiadacz koncesji przedkłada organowi nadzorczemu wyniki zatwierdzonych testów bezpieczeństwa informacji. Posiadacz koncesji nie może rozpocząć prowadzenia gier hazardowych, dopóki nie przejdzie pomyślnie testów bezpieczeństwa. Wynik testu bezpieczeństwa informacji nie może być starszy niż dwa lata.

Organ nadzorczy może, według własnego uznania, przyznać dodatkowy czas na przeprowadzenie testów bezpieczeństwa, podczas którego można kontynuować prowadzenie gier hazardowych.

6 Odrzucony test bezpieczeństwa informacji

Organ kontrolny przeprowadzający badanie bezpieczeństwa informacji powinien ocenić słabe punkty zidentyfikowane podczas badania bezpieczeństwa informacji i ich znaczenie dla niezawodności systemu gier hazardowych. Podatności zidentyfikowane podczas oceny należy oceniać za pomocą kalkulatora CVSS v3 (Common Vulnerability Scoring System Calculator version 3) udostępnionego przez Narodowy Instytut Technologii (NIST). W przypadku kalkulatora CVSS v3 dotkliwość podatności ocenia się za pomocą wskaźników bazowej oceny punktowej. Jeśli podczas testów bezpieczeństwa zostaną wykryte luki o obliczonej wartości CVSS wyższej niż 5,0, test nie może zostać uznany za udany.

Jeżeli test bezpieczeństwa informacji przeprowadzony przez posiadacza koncesji nie zostanie zatwierdzony, posiadacz koncesji musi niezwłocznie podjąć środki w celu usunięcia stwierdzonych luk w bezpieczeństwie informacji. Posiadacz koncesji zgłasza organowi nadzorczemu odrzucony test bezpieczeństwa informacji.

Posiadacz koncesji musi przeprowadzić nowy test bezpieczeństwa w ciągu 90 dni od odrzucenia testu bezpieczeństwa informacji. Nie ma potrzeby przeprowadzania ponownych testów bezpieczeństwa informacji w całym systemie gier hazardowych; zamiast tego testy bezpieczeństwa informacji mogą być ukierunkowane na niedociągnięcia, które spowodowały odrzucenie. W związku z ponownym testowaniem bezpieczeństwa informacji organ kontrolny musi upewnić się, że luki w zabezpieczeniach, które wcześniej były powodem do odrzucenia, zostały naprawione.

Wprowadzenie gier losowych nie może rozpocząć się przed przeprowadzeniem zatwierdzonego i ważnego testu bezpieczeństwa.

7 Skanowanie podatności na zagrożenia

Oprócz testów bezpieczeństwa posiadacze koncesji są zobowiązani do monitorowania bezpieczeństwa własnych systemów za pomocą regularnych skanów podatności. Celem skanowania podatności jest zapewnienie, że systemy hazardowe używane przez posiadacza koncesji nie mają żadnych zewnętrznych luk w zabezpieczeniach, które mogłyby zostać wykorzystane do przeprowadzenia ataków na systemy hazardowe.

Posiadacz koncesji jest zobowiązany do przeprowadzania raz w roku zewnętrznego skanowania podatności i zgłaszania wyników organowi nadzorczemu. Skanowanie podatności może być przeprowadzane przez zewnętrzny organ kontrolny akredytowany zgodnie z ISO/IEC 17025, ISO/IEC 17065 lub ISO/IEC 17020, jak określono w ust. 2 niniejszego rozporządzenia.

Posiadacz koncesji jest zobowiązany do usunięcia luk wykrytych podczas skanowania pod kątem luk w zabezpieczeniach za pomocą aktualizacji lub innych pilnych środków ograniczających ryzyko, jeżeli aktualizacje korygujące nie są dostępne. Metodę oceny opisaną w sekcji 6 stosuje się do luk w zabezpieczeniach wykrytych podczas skanowania pod kątem luk w zabezpieczeniach. Jeżeli obliczona wartość CVSS zidentyfikowanej podatności zewnętrznej przekracza 5,0, posiadacz koncesji podejmuje natychmiastowe działania w celu usunięcia podatności.

Organ kontrolny odpowiedzialny za przeprowadzenie skanowania podatności oraz jego personel muszą posiadać kompetencje i kwalifikacje niezbędne do przeprowadzenia testów. Niezbędne kompetencje do przeprowadzania skanów podatności można wykazać między innymi poprzez wcześniejsze doświadczenie zawodowe w zakresie testowania bezpieczeństwa informacji, doświadczenie w korzystaniu ze skanerów podatności, szkolenia lub powszechnie uznawane certyfikaty branżowe. Posiadacz koncesji jest zobowiązany do zapewnienia, aby osoby przeprowadzające testy posiadały kwalifikacje do wykonywania skanowania pod kątem podatności oraz, na żądanie, do wykazania swoich kwalifikacji.

Należy wyznaczyć osobę odpowiedzialną za przeprowadzenie skanowania podatności, aby zapewnić jego prawidłowe wykonanie. Ostateczna wersja sprawozdania ze skanowania pod kątem podatności jest podpisywana i zatwierdzana przez osobę odpowiedzialną oraz przekazywana organowi nadzorczemu.

8 Skanowanie podatności przeprowadzane w związku z testowaniem bezpieczeństwa informacji

Posiadacz koncesji może przeprowadzać skanowanie pod kątem podatności w ramach testów bezpieczeństwa informacji. Do skanowań pod kątem luk w zabezpieczeniach wykonywanych w ramach testów bezpieczeństwa informacji mają zastosowanie te same wymogi co do innych skanowań pod kątem luk w zabezpieczeniach.

9 Usuwanie luk bezpieczeństwa

Posiadacz koncesji jest zobowiązany do regularnego monitorowania bezpieczeństwa informacji w swoich własnych systemach gier hazardowych, nawet poza testami bezpieczeństwa informacji, oraz do usuwania luk w zabezpieczeniach, które zagrażają wiarygodności, gdy dostępne są poprawki lub inne metody ograniczania ryzyka.

Jeżeli nie jest możliwe szybkie usunięcie słabych punktów, posiadacz koncesji stara się wykorzystać dostępne środki w celu zwalczenia słabych punktów i zminimalizowania ich wpływu.

Jeżeli wartość oceny punktowej CVSS v3 wykrytej podatności zewnętrznej jest niższa niż 5,0, posiadacz koncesji może skorzystać z przysługującej mu swobody uznania przy wprowadzaniu korekt i ocenie pilności potrzeby ich wprowadzenia.

10 Korzystanie z wydanych certyfikatów

Akredytowany organ kontrolny zatwierdzony przez organ nadzorczy odpowiedzialny za przeprowadzanie testów bezpieczeństwa informacji lub skanowania luk w zabezpieczeniach może w ramach swojej kontroli wykorzystywać certyfikaty lub inne poświadczenia wydane posiadaczowi koncesji na oprogramowanie do gier hazardowych. Jeżeli organ kontrolny wykorzystuje istniejące certyfikaty w ramach kontroli, musi ocenić, czy certyfikaty te można uznać za wystarczająco wiarygodne dowody wiarygodności i bezpieczeństwa informacji systemu gier hazardowych posiadacza koncesji na oprogramowanie do gier hazardowych.

11 Odstępstwa

Posiadacz koncesji jest zobowiązany do niezwłocznego zgłaszania organowi nadzorczemu wszelkich wykrytych naruszeń bezpieczeństwa informacji lub ochrony danych, jeżeli istnieją powody, aby podejrzewać, że naruszono niezawodność systemów gier hazardowych lub sprzętu do loterii wykorzystywanych przez posiadacza koncesji.

Posiadacze koncesji nie są zobowiązani do zgłaszania organowi nadzorczemu ds. gier hazardowych drobnych incydentów związanych z bezpieczeństwem lub ochroną danych, jeżeli szacowana skuteczność incydentu jest ograniczona lub jeżeli incydent nie został oceniony jako mający znaczący wpływ na niezawodność systemów gier hazardowych.

12 Wejście w życie

Niniejsze rozporządzenie wchodzi w życie z dniem X [miesiąc] 2026 r.

Krajowa Rada Policji
Administracja ds. gier hazardowych
Konepajankatu 2, PL 50, 11101 Riihimäki
Tel. +358 295 480 181, poliisi.fi