

GLI-NORMEN-SERIE

GLI-19:

NORMEN FÜR INTERAKTIVE SPIELSYSTEME

VERSION: 3.0

REVISIONSDATUM: 17. JULI 2020



Über diese Norm

Diese technische Norm wurde von **Gaming Laboratories International, LLC (GLI)** entwickelt, um unabhängige technische Analysen und/oder Zertifizierungen für Branchenbeteiligte zu bieten, die den Status der Konformität von Spielbetrieb und -systemen mit den hierin dargelegten Anforderungen widerspiegeln.

Dieses Dokument ist für die Nutzung durch Regulierungsbehörden, Betreiber und Zulieferer als Compliance-Richtlinie für Technologien und Verfahrensweisen in Verbindung mit interaktiven Spielen vorgesehen. Diese Norm soll keine präskriptiven Anforderungen darstellen, die von jedem interaktiven Spielsystem und jedem Betreiber zu erfüllen sind; jedoch etabliert sie einen Standard bezüglich der Technologien und Verfahrensweisen zur Unterstützung dieses Betriebs.

Von Betreibern und Zulieferern wird erwartet, dass sie eine interne Kontrolldokumentation, Zugangsdaten und den zugehörigen Zugang zu einer mit einer Produktionsumgebung vergleichbaren Testumgebung bereitstellen, die gemäß dieser technischen Norm bewertet werden soll. Nach Abschluss der Tests stellt GLI eine Konformitätsbescheinigung aus, die als Nachweis der Zertifizierung gemäß dieser Norm dient.

GLI-19 sollte als dynamisches Dokument angesehen werden, das eine Anleitung liefert, die bei neuen Spiel- und Prozessimplementierungen an die Branchenentwicklungen angepasst wird.



Inhaltsverzeichnis

Chapter 1: Einführung in interaktive Spielsysteme	5
1.1 Einleitung.....	5
1.2 Anerkennung anderer zu Rate gezogener Normen.....	5
1.3 Gegenstand technischer Normen.....	6
1.4 Andere Anwendbare Dokumente	7
1.5 Interpretation dieses Dokuments.....	7
1.6 Prüfung und Audit.....	8
Chapter 2: Plattform-/Systemanforderungen	9
2.1 Einleitung.....	9
2.2 Systemuhr-Anforderungen.....	9
2.3 Kontrollprogramm-Anforderungen.....	9
2.4 Spielverwaltung.....	10
2.5 Spielerkontenverwaltung.....	11
2.6 Spieler-Software.....	15
2.7 Standort-Anforderungen	17
2.8 Aufzubewahrende Informationen	19
2.9 Berichtsanforderungen.....	25
Chapter 3: Anforderungen an Zufallszahlengenerator (RNG).....	28
3.1 Einleitung.....	28
3.2 Allgemeine RNG-Anforderungen.....	28
3.3 RNG-Stärke und -Überwachung.....	30
3.4 Mechanischer RNG (physisches Zufallsgerät)	30
Chapter 4: Spielanforderungen	33
4.1 Einleitung.....	33
4.2 Spielerschnittstelle.....	33
4.3 Spielsitzungs-Anforderungen.....	34
4.4 Spielinformationen und Spielregeln	36
4.5 Spielergebnis durch Zufallszahlengenerator (RNG)	43
4.6 Spiel-Fairness	44
4.7 Spielauszahlungs-Raten, Wahrscheinlichkeiten und Nicht-Cash-Prämien	45
4.8 Bonus-/Feature-Anforderungen	47
4.9 Alternative Spielmodi	50
4.10 Spiele mit Fähigkeitselementen.....	51
4.11 Peer-to-Peer (P2P)-Spiele.....	54
4.12 Persistenz-Spiele.....	55

4.13	Progressive Jackpots und stufenweise Jackpots.....	56
4.14	Spielrekonstruktion.....	59
4.15	Deaktivierungs-Anforderungen.....	59
4.16	Unterbrochene Spiele.....	60
4.17	Wetten auf virtuelle Ereignisse.....	61
4.18	Live-Spiel-Anforderungen.....	61
Appendix A : Betriebs-Audit für Gaming-Verfahrensweisen und -Praktiken		65
A.1	Einleitung.....	65
A.2	Interne Kontrollverfahren	65
A.3	Spielerkonto-Kontrollen	66
A.4	Allgemeine Betriebsabläufe.....	72
A.5	Spielregeln und -inhalte.....	74
A.6	Verfahren und Kontrollen für Glücksspiele	77
A.7	Verfahren und Kontrollen für „Peer-to-Peer (P2P)“-Spielsitzungen	79
A.8	Kontrollverfahren.....	80
Appendix B : Betriebs-Audit für technische Sicherheitskontrollen.....		82
B.1	Einleitung.....	82
B.2	Betrieb und Sicherheit des Systems.....	82
B.3	Datenintegrität.....	88
B.4	Kommunikation.....	92
B.5	Drittdienstleister.....	95
B.6	Technische Kontrollen.....	96
B.7	Fernzugriff und Firewalls.....	99
B.8	Änderungsmanagement.....	101
B.9	Sicherheitstechnische Überprüfung.....	102
Appendix C : Betriebs-Audit für Dienstleistungsanbieter		105
C.1	Einleitung.....	105
C.2	Dienstleistungen zur Informationssicherheit.....	105
C.3	Cloud-Dienste	107
C.4	Zahlungsdienste	108
C.5	Standortdienste	109
C.6	Live-Spiel-Dienste.....	109
Glossar der wichtigsten Begriffe.....		116

Einführung in interaktive Spielsysteme

1.1 Einleitung

1.1.1 Allgemeines

Gaming Laboratories International, LLC (GLI) testet seit 1989 Gaming-Geräte. Im Laufe der Jahre hat GLI zahlreiche technische Normen entwickelt, die von Jurisdiktionen weltweit genutzt werden. In diesem Dokument, *GLI-19*, werden die technischen Normen für interaktive Spielsysteme dargelegt.

1.1.2 Dokumentenhistorie

Bei diesem Dokument handelt es sich um eine Zusammenstellung, die auf zahlreichen Normungsdokumenten weltweit basiert. Einige wurden von GLI verfasst, andere von Regulierungsbehörden der Branche mit Anregungen von unabhängigen Testlaboren sowie Betreibern, Entwicklern und Lieferanten interaktiver Spielsysteme. GLI hat für jedes dieser Normungsdokumente die spezifischen Regeln zusammengeführt, einige Regeln entfernt sowie andere aktualisiert, um sowohl die technologische Änderung als auch den Zweck der Aufrechterhaltung einer objektiven Norm widerzuspiegeln, die allgemeine regulatorische Zielsetzungen erreicht, ohne die technologische Innovation unnötig zu behindern. GLI führt nachstehend Behörden auf, deren Dokumente vor dem Verfassen dieser Norm geprüft wurden. Es ist Teil der Geschäftspolitik von GLI, dieses Dokument mit der zugesicherten Häufigkeit zu aktualisieren, um Veränderungen hinsichtlich Technologie und/oder Prüfmethode widerzuspiegeln. Dieses Dokument wird kostenlos vertrieben und ist per Download auf der GLI-Website unter www.gaminglabs.com oder durch Kontaktaufnahme unter folgender Anschrift erhältlich:

Gaming Laboratories International, LLC.

600 Airport Road

Lakewood, NJ 08701

Telefon: (732) 942-3999

Fax: (732) 942-0043

1.2 Anerkennung anderer zu Rate gezogener Normen

1.2.1 Allgemeines

Diese technische Norm wurde unter Einbeziehung und teilweiser Übernahme von Dokumenten der nachstehend aufgeführten Organisationen entwickelt. GLI möchte den Regulierungsbehörden und anderen Branchenvertretern, die diese Dokumente zusammengestellt haben, seine Anerkennung und seinen Dank aussprechen:

- a) Nevada Gaming Commission and Gaming Control Board.
- b) British Columbia Gaming Policy and Enforcement Branch (GPEB).
- c) Tasmanian Liquor and Gaming Commission.

- d) Danish Gambling Authority.
- e) Spanish Directorate General for the Regulation of Gambling (DGOJ).
- f) Alderney Gambling Control Commission.
- g) Lottery and Gaming Authority, Malta.
- h) United Kingdom Gambling Commission.
- i) World Lottery Association (WLA).

1.3 Gegenstand technischer Normen

1.3.1 Allgemeines

Diese technische Norm dient folgenden Zwecken:

- a) Beseitigen subjektiver Kriterien bei der Analyse und Zertifizierung interaktiver Spielsysteme.
- b) Überprüfen der Kriterien, die sich auf die Vertrauenswürdigkeit und Integrität interaktiver Spielsysteme hinsichtlich der Umsatzgenerierung sowie der Perspektive des Spielers auswirken.
- c) Entwickeln einer Norm zur Sicherstellung, dass interaktives Spielen fair, sicher sowie überprüfbar ist und korrekt betrieben wird.
- d) Unterscheidung zwischen Kriterien der lokalen öffentlichen Ordnung und Kriterien unabhängiger Prüflabore. Es ist Aufgabe der einzelnen lokalen Jurisdiktionen, ihre eigenen öffentlichen Gaming-Richtlinien zu definieren.
- e) Anerkennen, dass die Beurteilung interner Kontrollsysteme (wie Geldwäschebekämpfung, Finanz- und Geschäftsprozesse) der Betreiber des interaktiven Spielsystems nicht in die Laborprüfungen der Norm eingeschlossen ist, sondern stattdessen Teil der Betriebsprüfungen für lokale Jurisdiktionen ist.
- f) Entwickeln einer Norm, die einfach überarbeitet werden kann, um neue Technologien zu berücksichtigen.
- g) Entwickeln einer Norm, die kein bestimmtes Konzept, keine Methode und keinen Algorithmus spezifiziert. Ziel ist es, die Nutzung eines breiten Spektrums von Methoden zur Herstellung einer Normenkonformität zu ermöglichen und gleichzeitig die Entwicklung neuer Methoden zu fördern.

1.3.2 Keine Technologiebeschränkungen

Es sei darauf hingewiesen, dass dieses Dokument nicht auf eine Weise auszulegen ist, die eine Nutzung zukünftiger Technologien einschränkt. Dieses Dokument sollte nicht so interpretiert werden, dass nicht erwähnte Technologien nicht zulässig sind. Stattdessen wird GLI diese Norm überprüfen und Änderungen vornehmen, um Mindest-Standards für alle neuen und zugehörigen Technologien zu integrieren.

1.3.3 Übernahme und Beachtung

Diese technische Norm kann vollständig oder teilweise von jeder Regulierungsbehörde übernommen werden, die umfassende Anforderungen für interaktive Spielsysteme implementieren möchte.

1.4 Andere Anwendbare Dokumente

1.4.1 Andere GLI-Normen

Diese technische Norm beinhaltet die Anforderungen für interaktive Spielsysteme. Abhängig von der durch ein System genutzten Technologie können weitere technische GLI-Normen anwendbar sein.

HINWEIS: Die gesamte Reihe von GLI-Normen ist kostenlos erhältlich unter www.gaminglabs.com.

1.4.2 Interne Mindest-Kontrollstandards (MICS)

Die Implementierung eines interaktiven Spielsystems ist eine komplexe Aufgabe und erfordert die Entwicklung interner Prozesse und Verfahrensweisen, um sicherzustellen, dass das System mit dem erforderlichen Mindestmaß an Sicherheit und Kontrolle konfiguriert und betrieben wird. Insofern wird erwartet, dass eine Reihe interner Mindest-Kontrollstandards (MICS) implementiert wird, um die internen Prozesse für die Verwaltung und Handhabung von Spielen sowie die Anforderungen für eine interne Kontrolle jeglicher System- oder Komponenten-Software oder -Hardware und der jeweiligen Verantwortlichkeiten zu definieren.

1.5 Interpretation dieses Dokuments

1.5.1 Allgemeines

Diese technische Norm ist auf Systeme anwendbar, die interaktives Spielen unterstützen, und soll allgemeiner Natur sein, ohne bestimmte Spielarten und Funktionalitäten zu begrenzen oder zu autorisieren. Ziel ist die Bereitstellung eines Rahmenwerks für bereits bekannte und gesetzlich zulässige Spielarten. Dieses Dokument soll nicht definieren, welche Parteien dafür verantwortlich sind, die Anforderungen im Rahmen dieser technischen Norm zu erfüllen. Es liegt in der Verantwortung der entsprechenden Beteiligten jedes Betreibers, die besten Möglichkeiten zur Erfüllung der in diesem Dokument dargelegten Anforderungen zu bestimmen.

HINWEIS: Diese technische Norm ist NICHT auf Systeme anwendbar, die Wetten auf Sportereignisse, Wettbewerbe, Begegnungen und andere Ereignisarten mithilfe eines Ereignis-Wettsystems unterstützen. Detaillierte, auf diese Systeme anwendbare Normen finden Sie in den *GLI-33 Normen für Ereignis-Wettsysteme*.

1.5.2 Software-Lieferanten und Betreiber

Die Komponenten eines interaktiven Spielsystems sind trotz eines modularen Aufbaus so konzipiert, dass sie nahtlos zusammenarbeiten. Darüber hinaus können interaktive Spielsysteme so entwickelt werden, dass sie konfigurierbare Funktionen aufweisen; die endgültige Konfiguration hängt von betreiberseitig gewählten Optionen ab. Bei Prüfungen ist es unter Umständen nicht möglich, alle konfigurierbaren Funktionen eines von einem Software-Lieferanten eingereichten interaktiven Spielsystems zu testen, ohne dass die endgültig vom Betreiber ausgewählte Konfiguration vorliegt; jedoch soll die in der Produktionsumgebung verwendete Konfiguration dem unabhängigen Prüflabor mitgeteilt werden, um den Aufbau einer Testumgebung mit vergleichbarer Funktionalität zu ermöglichen. Aufgrund der integrierten Natur eines interaktiven Spielsystems sind mehrere

Anforderungen in diesem Dokument sowohl auf Betreiber als auch auf Lieferanten anwendbar. In diesen Fällen, wenn die Prüfung für eine „White-Label“-Version des Systems erfolgen soll, wird eine bestimmte Konfiguration getestet und hierzu ein Bericht erstellt.

1.6 Prüfung und Audit

1.6.1 Laborprüfung

Das unabhängige Prüflabor prüft und zertifiziert ggf. die Komponenten des interaktiven Spielsystems in Übereinstimmung mit den Kapiteln dieser technischen Norm innerhalb einer kontrollierten Prüfumgebung. Alle diese Anforderungen, die zusätzliche betriebliche Verfahrensweisen bedingen, um die Anforderungen zu erfüllen, müssen innerhalb des Beurteilungsberichts dokumentiert und zur Ergänzung des Umfangs des Betriebs-Audits verwendet werden.

1.6.2 Betriebs-Audit

Die Integrität und Genauigkeit des Betriebs eines interaktiven Spielsystems ist hochgradig abhängig von betrieblichen Verfahrensweisen, Konfigurationen und der Netzwerk-Infrastruktur der Produktionsumgebung. Ein Betriebs-Audit ist eine unverzichtbare Ergänzung der Prüfung und Zertifizierung eines interaktiven Spielsystems. Das in den folgenden Anhängen dieser technischen Norm dargelegte Betriebs-Audit soll in einer durch die Regulierungsbehörde definierten Häufigkeit durchgeführt werden:

- a) Anhang A: Betriebs-Audit für Gaming-Verfahrensweisen und -Praktiken. Dies beinhaltet beispielsweise die Prüfung der internen Kontrollen, Verfahrensweisen und Praktiken für den Spielbetrieb, wie beispielsweise Definieren von Spielregeln, Verwalten von Spielen, Abwickeln verschiedener Spiel- und Finanz-Transaktionen, Erstellen und Verwalten progressiver Jackpots, Erstellen und Verwalten stufenweiser Jackpots, Spielerkontenverwaltung, grundlegende, für die Risikobegrenzung relevante Praktiken sowie jegliche andere Zielsetzungen, die von der Regulierungsbehörde definiert wurden.
- b) Anhang B: Betriebs-Audit für technische Sicherheitskontrollen. Dies beinhaltet beispielsweise eine Prüfung der betrieblichen Prozesse, die wichtig für die Compliance sind, Penetrationstests mit Schwerpunkt auf externer und interner Infrastruktur sowie Anwendungen, die personenbezogene Daten (PII) und/oder sensible Daten übertragen, speichern und/oder verarbeiten sowie jegliche anderen von der Regulierungsbehörde definierten Zielsetzungen.
- c) Anhang C: Betriebs-Audit für Dienstleister. Dies beinhaltet beispielsweise die Bewertung von Anbietern bestimmter Dienste, die direkt durch den Betreiber angeboten werden können oder die Beteiligung von Drittanbietern beinhalten, wie beispielsweise die Beurteilung von Informationssicherheits-Diensten, Cloud-Services, Zahlungsdienste (Finanzinstitute, Zahlungsabwickler etc.), Standortdienste, Live-Game-Services und jegliche andere Dienste, die direkt vom Betreiber angeboten werden oder die Beteiligung von Drittanbietern beinhalten können.

Chapter 2: Plattform-/Systemanforderungen

2.1 Einleitung

2.1.1 Allgemeines

Wenn das interaktive Spielsystem aus mehreren Computersystemen an unterschiedlichen Standorten besteht, sollen das System insgesamt sowie jegliche Kommunikation zwischen seinen Komponenten den anwendbaren technischen Anforderungen in diesem Dokument entsprechen.

2.2 Systemuhr-Anforderungen

2.2.1 Systemuhr

Das interaktive Spielsystem muss über eine interne Uhr verfügen, die das aktuelle Datum und die aktuelle Uhrzeit wiedergibt, um für Folgendes genutzt zu werden:

- a) Zeitstempel aller Transaktionen und Spiele;
- b) Zeitstempel signifikanter Ereignisse; und
- c) Referenzuhr für die Berichtserstellung.

2.2.2 Zeitsynchronisierung

Das interaktive Spielsystem muss über einen Mechanismus verfügen, der gewährleistet, dass die Uhrzeit und das Datum zwischen allen Komponenten, aus denen System besteht, korrekt synchronisiert und eingestellt werden.

2.3 Kontrollprogramm-Anforderungen

2.3.1 Allgemeines

Neben den Anforderungen in diesem Abschnitt sind auch die Anforderungen im Abschnitt „Verifizierungsverfahren“ dieses Dokuments zu erfüllen.

2.3.2 Selbstverifizierung des Kontrollprogramms

Das interaktive Spielsystem muss in der Lage sein, zu verifizieren, dass es sich bei allen im System enthaltenen kritischen Kontrollprogramm-Komponenten um authentische Kopien der genehmigten Systemkomponenten handelt. Diese Prüfung erfolgt mindestens alle vierundzwanzig Stunden sowie bei Bedarf mithilfe einer von der Regulierungsbehörde genehmigten Methode. Die kritischen Authentifizierungs-Mechanismen des Kontrollprogramms müssen:

- a) einen kryptographischen Hash-Algorithmus nutzen, der einen Hashwert von mindestens 128 Bit erzeugt. Andere Prüfmethode müssen auf fallweiser Basis beurteilt werden;

- b) alle kritischen Kontrollprogramm-Komponenten beinhalten, die sich auf den Spielbetrieb auswirken können, wie beispielsweise ausführbare Dateien, Spiel- oder Systemkonfigurationen, Betriebssystem-Dateien, Komponenten zur Steuerung der erforderlichen Systemberichte sowie Datenbankelemente, die sich auf den Systembetrieb auswirken; und
- c) einen Hinweis auf den Authentifizierungsfehler liefern, falls sich eine kritische Komponente des Kontrollprogramms als ungültig erweist.

2.3.3 Unabhängige Verifizierung des Kontrollprogramms

Jede kritische Programmkomponente des interaktiven Spielsystems muss über eine Methode zur Verifizierung durch ein unabhängiges Drittpartei-Prüfverfahren verfügen. Das Drittpartei-Prüfverfahren muss unabhängig von Prozess- oder Sicherheits-Software innerhalb des Systems durchlaufen werden. Das unabhängige Prüflabor muss vor der Genehmigung des Systems die Methode zur Integritätsprüfung beurteilen.

2.4 Spielverwaltung

2.4.1 Spielverwaltung

Das interaktive Spielsystem muss in der Lage sein, auf Anforderung Folgendes zu deaktivieren:

- a) jegliche Spielaktivität;
- b) einzelne Spielthemen/Gewinntabellen oder Versionen (z. B. Desktop, Mobilgerät, Tablet etc.); und
- c) Logins einzelner Spieler.

2.4.2 Änderungen an Jackpot-Parametern

Die folgenden Anforderungen gelten für die Änderung der Parameterwerte progressiver Jackpots oder stufenweiser Jackpots, nachdem die aktuelle Jackpot-Auszahlung bereits Spielerbeiträge aufwies und ohne Notwendigkeit einer Außerkraftsetzung:

- a) Bei Jackpots mit einer konfigurierbaren Erhöhungsrate, die sich auf die Auszahlungsquote (RTP) des Spiels/der Spiele auswirkt, können Änderungen der Erhöhungsrate nicht wirksam werden, bis der aktuelle Jackpot gewonnen wird;
- b) bei Jackpots mit einer konfigurierbaren Deckelung, die sich nicht auf die RTP des Spiels/der Spiele auswirkt, können Änderungen der Deckelung nur für einen Wert erfolgen, der höher ist als die aktuelle Auszahlung. Alternativ können Änderungen der Deckelung nicht wirksam werden, bis der aktuelle Jackpot gewonnen wird;
- c) Änderungen an den Parametern dürfen sich nicht auf die Wahrscheinlichkeiten für das Auslösen des aktuellen Jackpots auswirken;
- d) bei Jackpots mit Mystery-Auslösung, die einen verborgenen Auslösungsbetrag nutzen, um den Jackpot-Gewinn zu bestimmen:
 - i. Der verborgene Auslösungsbetrag muss neu gewählt werden, wenn jegliche Parameter geändert werden, die zu einem unmittelbaren Auslösen aufgrund der Änderung führen; und

- ii. der neu gewählte Betrag muss im Bereich zwischen der aktuellen Auszahlung und der Deckelung liegen und darf nach der Änderung nicht zu einem Auslösen ohne jegliche Beteiligung führen.

2.4.3 Jackpot-Änderungen

Das interaktive Spielsystem muss ein sicheres Hilfsmittel zum Übertragen oder Kombinieren von Beiträgen aus einem außer Kraft gesetzten Jackpot (und jeglicher spezieller Überschuss- oder Umleitungspools für diesen Jackpot) beinhalten, um Fehler bei einem Jackpot zu korrigieren oder um andere Anforderungen der Regulierungsbehörde zu erfüllen.

2.5 Spielerkontenverwaltung

2.5.1 Allgemeines

Das interaktive Spielsystem erfordert von einem Spieler die Registrierung und Verifizierung eines Kontos, um an interaktiven Spielen teilnehmen zu können. Neben den Anforderungen in diesem Abschnitt sind auch die Anforderungen im Abschnitt „Spielerkonto-Kontrollen“ dieses Dokuments zu erfüllen.

2.5.2 Registrierung und Verifizierung

Vor der Registrierung eines Spielerkontos soll eine Methode zur Erfassung der personenbezogenen Daten (PII) des Spielers genutzt werden. Wenn die Registrierung und Verifizierung eines Spielerkontos vom interaktiven Spielsystem entweder direkt durch das System oder in Verbindung mit der Software eines Drittanbieters unterstützt werden, sind die folgenden Anforderungen zu erfüllen:

- a) Nur Spieler, die das gesetzlich vorgeschriebene Mindestalter für das Spielen innerhalb der jeweiligen Jurisdiktion erreicht haben, können ein Spielerkonto registrieren. Während des Registrierungsvorgangs muss der Spieler:
 - i. keine Möglichkeit zur Registrierung eines Spielerkontos erhalten, wenn er ein Geburtsdatum übermittelt, das darauf hindeutet, dass er das erforderliche Mindestalter noch nicht erreicht hat;
 - ii. auf dem Registrierungsformular darüber informiert werden, bei welchen Feldern es sich um „Pflichtfelder“ handelt und bei welchen nicht, und welche Folgen entstehen, wenn die Pflichtfelder nicht ausgefüllt sind;
 - iii. den allgemeinen Geschäftsbedingungen sowie der Datenschutzrichtlinie zustimmen;
 - iv. bestätigen, dass es ihm nicht gestattet ist, jeglichen nicht autorisierten Personen den Zugriff auf oder die Nutzung ihres Spielerkontos zu erlauben;
 - v. der Überwachung und Aufzeichnung von Informationen in Bezug auf die Nutzung ihres Spielerkontos durch den Betreiber und die Regulierungsbehörde zustimmen; und
 - vi. versichern, dass die vom Spieler angegebenen personenbezogenen Daten (PII) korrekt sind.
- b) Eine Identitätsprüfung muss durchgeführt werden, bevor dem Spieler gestattet wird, an einem Spiel teilzunehmen. Es können Drittanbieter zur Identitätsprüfung eingesetzt werden, soweit die Regulierungsbehörde dies gestattet.

- i. Die Identitätsprüfung muss gemäß den Anforderungen der Regulierungsbehörde mindestens den offiziellen Namen, die Wohnadresse sowie das Geburtsdatum der Einzelperson bestätigen.
 - ii. Die Identitätsprüfung muss ebenfalls bestätigen, dass der Spieler nicht auf einer Ausschlussliste des Betreibers oder der Regulierungsbehörde geführt wird oder aus anderen Gründen kein Konto eröffnen oder besitzen darf.
 - iii. Die Details der Identitätsprüfung sind auf sichere Weise aufzubewahren.
- c) Das Spielerkonto kann nur aktiv werden, nachdem die Alters- und Identitätsprüfung erfolgreich abgeschlossen wurden und ermittelt wurde, dass der Spieler auf keinerlei Ausschlusslisten geführt wird, oder aus anderen Gründen kein Konto eröffnen oder besitzen darf. Nachdem der Spieler darüber hinaus den erforderlichen Geschäftsbedingungen sowie der Datenschutzrichtlinie zugestimmt hat, ist die Registrierung des Spielerkontos abgeschlossen.
 - d) Einem Spieler darf nur gestattet werden, zeitgleich ein aktives Konto zu besitzen, sofern von der Regulierungsbehörde keine anderweitige ausdrückliche Autorisierung vorliegt.
 - e) Das System muss für jeden Spieler die Aktualisierung der Authentifizierungsdaten, der Registrierungsinformationen sowie des für die Finanztransaktionen verwendeten Kontos ermöglichen. Für diese Zwecke muss eine Multifaktor-Authentifizierung implementiert werden.

2.5.3 Spielerzugriff

Ein Spieler greift mithilfe von Authentifizierungsdaten wie einem Benutzernamen (oder Ähnlichem) und einem Passwort oder mithilfe sicherer Alternativen auf sein Spielerkonto zu, um sich von einem bestimmten Remote-Spieler-Gerät im interaktiven Spielsystem anzumelden. Zulässige Authentifizierungsdaten unterliegen nach Bedarf dem Ermessen der Regulierungsbehörde. Die Anforderung verbietet nicht die Möglichkeit, einem Spieler mehr als eine Authentifizierungsmethode für den Zugriff auf sein Konto zur Verfügung zu stellen.

- a) Wenn das System die Authentifizierungsdaten bei der Eingabe nicht erkennt, muss dem Spieler eine erklärende Meldung angezeigt werden, in der er zu einem erneuten Versuch aufgefordert wird. Die Fehlermeldung muss gleich lauten, unabhängig davon, welche Authentifizierungsdaten inkorrekt sind.
- b) Wenn ein Spieler seine Authentifizierungsdaten vergessen hat, muss ein Multifaktor-Authentifizierungsprozess eingesetzt werden, um die vergessenen Authentifizierungsdaten wiederherzustellen oder zurückzusetzen.
- c) Nach der Authentifizierung müssen dem Spieler aktuelle Informationen zum Kontostand zur Verfügung gestellt werden, einschließlich jeglicher Anreizgutschriften. Alle eingeschränkten Anreizgutschriften und Anreizgutschriften mit einem möglichen Ablaufdatum müssen separat angegeben werden.
- d) Das System muss einen Mechanismus unterstützen, der die Sperrung eines Kontos ermöglicht, wenn verdächtige Aktivitäten erkannt werden, wie beispielsweise drei fehlgeschlagene Anmeldungen in Folge innerhalb von dreißig Minuten. Zum Entsperren des Kontos muss eine Multifaktor-Authentifizierung implementiert werden.

HINWEIS: Wenn Passwörter als Authentifizierungsdaten genutzt werden, wird für diese eine Länge von mindestens acht Zeichen empfohlen.

2.5.4 Spieler-Inaktivität

Nach dreißig Minuten Inaktivität auf diesem Remote-Spieler-Gerät oder nach Verstreichen eines von der Regulierungsbehörde bestimmten Zeitraums muss der Spieler sich erneut authentifizieren, um auf sein Spielerkonto zuzugreifen.

- a) Auf diesem Gerät sind keine weiteren Spiele oder Finanztransaktionen mehr gestattet, bis der Spieler erneut authentifiziert wurde.
- b) Dem Spieler kann eine einfachere Möglichkeit zur erneuten Authentifizierung auf diesem Gerät angeboten werden, wie beispielsweise eine Authentifizierung auf Betriebssystemebene (z. B. biometrisch) oder mithilfe einer persönlichen Identifikationsnummer (PIN). Alle Hilfsmittel für eine erneute Authentifizierung werden auf fallweiser Basis durch das unabhängige Prüflabor beurteilt.
 - i. Diese Funktion kann aufgrund der Präferenzen des Spielers und/oder auf Verlangen der Regulierungsbehörde deaktiviert sein.
 - ii. Einmal alle dreißig Tage oder innerhalb eines von der Regulierungsbehörde festgelegten Zeitraums muss der Spieler eine vollständige Authentifizierung auf diesem Gerät durchführen.

2.5.5 Einschränkungen und Ausschlüsse

Das interaktive Spielsystem muss in der Lage sein, jegliche Einschränkungen und/oder Ausschlüsse, die durch den Spieler und/oder Betreiber in Kraft gesetzt wurden, gemäß den Anforderungen der Regulierungsbehörde korrekt zu implementieren:

- a) Wo das System die Möglichkeit bietet, Einschränkungen und/oder Ausschlüsse direkt zu verwalten, müssen die anwendbaren Verpflichtungen innerhalb der Abschnitte „Einschränkungen“ und „Ausschlüsse“ dieses Dokuments beurteilt werden;
- b) die selbst auferlegten Einschränkungen durch einen Spieler dürfen keine durch den Betreiber eingesetzten restriktiveren Einschränkungen außer Kraft setzen. Die restriktiveren Einschränkungen müssen Priorität genießen; und
- c) Einschränkungen dürfen nicht durch interne Statusereignisse wie selbst auferlegte Ausschlüsse und Widerrufe kompromittiert werden.

2.5.6 Finanztransaktionen

Wenn Finanztransaktionen automatisch vom interaktiven Spielsystem durchgeführt werden können, müssen die folgenden Anforderungen erfüllt werden:

- a) Das System muss eine Bestätigung/Ablehnung jeder initiierten Finanztransaktion bereitstellen, einschließlich
 - i. der Art der Transaktion (Einzahlung/Auszahlung);
 - ii. des Transaktionswerts; und
 - iii. bei abgelehnten Transaktionen eine beschreibende Mitteilung, warum die Transaktion nicht wie initiiert durchgeführt wurde.

- b) Eine Einzahlung auf ein Spielerkonto mithilfe einer Lastschrift-Transaktion, Kreditkarten-Transaktion oder anderer Methoden, die eine ausreichende Protokollierung ermöglichen.
- c) Es darf kein Geld für Wetten zur Verfügung stehen, bis es vom Aussteller empfangen wurde oder der Aussteller eine Autorisierungsnummer bereitstellt, die belegt, dass es sich um autorisierte Geldmittel handelt. Die Autorisierungsnummer wird in einem Prüfprotokoll gespeichert.
- d) Zahlungen von einem Konto (einschließlich Geldüberweisung) sind direkt an ein Konto zu leisten, das bei einem Finanzinstitut im Namen des Spielers geführt wird, oder an den Spieler zahlbar zu stellen und mithilfe eines sicheren Zustelldienstes an seine Anschrift zu senden oder über eine andere, von der Regulierungsbehörde nicht untersagte Methode zu übermitteln. Der Name und die Anschrift müssen den bei der Spielerregistrierung angegebenen Daten entsprechen.
- e) Wenn ein Spieler eine Finanztransaktion initiiert und diese Transaktion durch den Betreiber und/oder die Regulierungsbehörde festgelegte Grenzwerte überschreiten würde, darf diese Transaktion nur durchgeführt werden, wenn der Spieler eine klar verständliche Nachricht erhält, dass die Auszahlung oder Einzahlung geringer ist als angefordert.
- f) Es darf nicht möglich sein, Geld zwischen Spielerkonten zu übertragen.

2.5.7 Transaktionsprotokoll oder Kontoauszug

Das interaktive Spielsystem muss in der Lage sein, einem Spieler auf Anforderung ein Transaktionsprotokoll oder einen Kontoauszugsverlauf bereitzustellen. Die bereitgestellten Informationen beinhalten ausreichende Informationen, um dem Spieler einen Abgleich des Auszugs oder Protokolls mit seinen eigenen Finanzaufzeichnungen zu ermöglichen. Die anzugebenden Informationen müssen mindestens Details zu den folgenden Arten von Transaktionen innerhalb des vergangenen Jahres oder eines anderen Zeitraums beinhalten, wie vom Spieler gewünscht oder von der Regulierungsbehörde gefordert:

- a) Finanztransaktionen (mit Zeitstempel mit einer eindeutigen Transaktions-ID):
 - i. Einzahlungen auf das Spielerkonto;
 - ii. Auszahlungen vom Spielerkonto;
 - iii. Anreizgutschriften, die dem Spielerkonto hinzugefügt wurden/aus dem Spielerkonto entfernt wurden (außer in Spielen gewonnene Gutschriften);
 - iv. manuelle Anpassungen oder Änderungen am Spielerkonto (z. B. aufgrund von Erstattungen);
 - v. jegliche nicht einsatzbezogenen Käufe (sofern zutreffend);
- b) Spielverlauf (nach Spielthema);
 - i. den Namen des Spielthemas und den Spieltyp (Automat, Blackjack, Poker, Tisch etc.);
 - ii. eingesetzter Gesamtbetrag, einschließlich jeglicher Anreizgutschriften (sofern zutreffend); und
 - iii. gewonnener Gesamtbetrag für abgeschlossene Spiele, einschließlich jeglicher Anreizgutschriften und/oder Preise sowie jeglicher progressiver Jackpots und/oder stufenweiser Jackpots (sofern zutreffend).

2.5.8 Spielertreueprogramme

Spielertreueprogramme sind alle Programme, die Anreizprämien für Spieler bieten, üblicherweise basierend auf dem Umfang der Spielaktivität oder den vom Spieler erhaltenen Einnahmen. Wenn

Spieler-treueprogramme vom interaktiven Spielsystem unterstützt werden, müssen die folgenden Grundsätze gelten:

- a) Alle Prämien müssen allen Spielern, die das festgelegte Qualifikationsniveau für Spieler-treuepunkte erreichen, auf gleiche Weise zur Verfügung stehen;
- b) das Einlösen von Spieler-treuepunkten muss durch eine sichere Transaktion erfolgen, die automatisch das Punkteguthaben um den Wert des eingelösten Preises reduziert; und
- c) alle Transaktionen in Verbindung mit Spieler-treuepunkten müssen vom System aufgezeichnet werden.

2.6 Spieler-Software

2.6.1 Allgemeines

Die Spieler-Software wird verwendet, um an Spielen teilzunehmen und Finanztransaktionen über das interaktive Spielsystem durchzuführen, das designbasiert auf das Remote-Spieler-Gerät heruntergeladen oder auf diesem installiert wird, vom interaktiven Spielsystem ausgeführt wird, auf das vom Remote-Spieler-Gerät oder einer Kombination aus beidem zugegriffen wird.

2.6.2 Software- Kennung

Die Spieler-Software muss ausreichende Informationen zur Identifizierung der Software und ihrer Version enthalten.

2.6.3 Software-Validierung

Bei Spieler-Software, die lokal auf dem Remote-Spieler-Gerät installiert ist, muss gemäß Anforderung der Regulierungsbehörde bei jedem Start der Software und, sofern vom System unterstützt, auf Anforderung eine Authentifizierung möglich sein, dass alle kritischen Software-Komponenten gültig sind. Kritische Software-Komponenten können beispielsweise Folgendes umfassen: Spielregeln, Auszahlungstabellen-Informationen, Elemente zur Steuerung der Kommunikation zwischen dem Remote-Spieler-Gerät und dem interaktiven Spielsystem oder anderen Software-Komponenten, die zur Sicherstellung eines ordnungsgemäßen Software-Betriebs erforderlich sind. Im Fall einer fehlgeschlagenen Authentifizierung (d. h. fehlende Übereinstimmung oder Authentifizierungsfehler) muss die Software Spielaktivitäten verhindern und eine entsprechende Fehlermeldung anzeigen.

HINWEIS: Die Mechanismen zur Programmverifizierung werden fallweise von der Regulierungsbehörde und dem unabhängigen Prüflabor beurteilt und basierend auf dem Branchenstandard entsprechenden Sicherheitspraktiken genehmigt.

2.6.4 Kommunikation

Die Spieler-Software muss so konzipiert oder programmiert sein, dass sie nur mit autorisierten Komponenten über sichere Kommunikationswege kommuniziert. Wenn die Kommunikation zwischen dem interaktiven Spielsystem und dem Remote-Spieler-Gerät abbricht, muss die Software weitere Spielaktivitäten verhindern und eine entsprechende Fehlermeldung anzeigen. Es ist zulässig,

dass die Software diesen Fehler erkennt, wenn das Gerät versucht, mit dem System zu kommunizieren.

2.6.5 Client-Server-Interaktionen

Der Spieler kann eine Anwendung oder ein Software-Paket erhalten/herunterladen, die/das die Spieler-Software enthält, oder per Browser auf die Software zugreifen, um über das interaktive Spielsystem an Spielaktivitäten teilzunehmen und Finanztransaktionen durchzuführen.

- a) Die Spieler dürfen keine Möglichkeit erhalten, die Software zu nutzen, um Daten auf andere Weise untereinander auszutauschen als über Chatfunktionen (z. B. Text, Sprache, Video etc.) sowie zulässige Dateien (z. B. Benutzerprofilbilder, Fotos etc.);
- b) die Software darf nicht automatisch jegliche Virens Scanner und/oder Erkennungsprogramme deaktivieren oder jegliche gerätespezifischen Firewall-Regeln ändern, um Ports zu öffnen, die entweder durch eine Hardware- oder Software-Firewall blockiert sind;
- c) die Software darf auf keinerlei TCP-/UDP-Ports zugreifen (weder automatisch noch durch Aufforderung des Benutzers zu manuellem Zugriff), die nicht zur Kommunikation zwischen Remote-Spieler-Gerät und Server erforderlich sind;
- d) wenn die Software über weitere nicht spielbezogene Funktionen verfügt, dürfen diese die Integrität der Software in keiner Weise beeinträchtigen;
- e) die Software darf nicht in der Lage sein, die Lautstärke-Einstellungen des Remote-Spieler-Geräts außer Kraft zu setzen;
- f) die Software darf nicht zur Speicherung sensibler Informationen verwendet werden. Es wird empfohlen, Funktionen wie automatische Vervollständigung, Passwort-Caching oder andere Methoden zum Ausfüllen des Passwortfeldes für die Software standardmäßig zu deaktivieren; und
- g) die Software darf keine Logik zum Generieren von Ergebnissen für jegliche Spiele enthalten. Alle kritischen Funktionen, einschließlich des Generierens jeglicher Spielergebnisse, müssen unabhängig vom Remote-Spieler-Gerät durch die Spielplattform bereitgestellt werden.

2.6.6 Verifizierung der Kompatibilität

Während jeder Installation oder Initialisierung und vor dem Beginn von Spielaktivitäten muss die in Verbindung mit dem interaktiven Spielsystem verwendete Spieler-Software jegliche Inkompatibilitäten oder Ressourceneinschränkungen des Remote-Spieler-Geräts erkennen, die einen ordnungsgemäßen Betrieb der Software verhindern würden (z. B. Software-Version, nicht erfüllte Mindestanforderungen, Browser-Typ, Browser-Version, Plug-in-Version etc.). Werden jegliche Inkompatibilitäten oder Ressourceneinschränkungen erkannt, muss die Software Spielaktivitäten verhindern und eine entsprechende Fehlermeldung anzeigen.

2.6.7 Software-Inhalte

Die Spieler-Software darf keinen Schadcode oder Funktionen enthalten, die von der Regulierungsbehörde als schädlich angesehen werden. Dies beinhaltet beispielsweise nicht autorisierte Extraktionen/Übertragungen, nicht autorisierte Gerätemodifikationen, nicht

autorisierten Zugriff auf jegliche lokal gespeicherten Informationen (z. B. Kontakte, Kalender etc.) und Malware.

2.6.8 Cookies

Wo Cookies verwendet werden, müssen die Spieler bei der Installation der Spieler-Software oder während der Spieler-Registrierung über die Cookie-Nutzung informiert werden. Wenn Cookies für die Spielabwicklung erforderlich sind, können keine Spielaktivitäten stattfinden, wenn die Cookies nicht durch das Remote-Spieler-Gerät akzeptiert werden. Keiner der verwendeten Cookies darf einen schädlichen Code enthalten.

2.6.9 Informationszugriff

Neben den „Spielanforderungen“ in diesem Dokument muss die Spieler-Software die in den folgenden Abschnitten dieses Dokuments angegebenen Elemente entweder direkt über die Spieler-Oberfläche oder über eine dem Spieler zugängliche Seite anzeigen:

- a) „Spielregeln und Inhalte“;
- b) „Informationen zum Spielerschutz“;
- c) „Geschäftsbedingungen“; und
- d) „Datenschutzrichtlinie“.

2.7 Standort-Anforderungen

2.7.1 Allgemeines

Die Anforderungen in diesem Abschnitt gelten für die Erkennung des Spieler-Standorts. Neben den in diesem Abschnitt enthaltenen Anforderungen muss der Betreiber oder für die Pflege dieser Komponenten, Services und/oder Anwendungen zuständige Drittanbieter den im Abschnitt „Standort-Services“ dieses Dokuments angegebenen betrieblichen Verfahrensweisen und Kontrollen entsprechen.

2.7.2 Standortbetrugs-Prävention

Das interaktive Spielsystem muss einen Mechanismus beinhalten, der die Nutzung von Remote-Desktop-Software, Rootkits, Virtualisierung und/oder anderen Programmen erkennt, die für ihre Fähigkeit bekannt sind, die Standorterkennung zu umgehen. Dies muss mithilfe von Best-Practice-Sicherheitsmaßnahmen erfolgen, um:

- a) Standortdaten-Betrug (z. B. Fake-Standort-Anwendungen, virtuelle Maschinen, Remote-Desktop-Programme etc.) vor der Initiierung jedes Spiels zu erkennen und zu blockieren;
- b) die IP-Adresse bei jeder Verbindung des Remote-Spieler-Geräts zu einem Netzwerk zu untersuchen, um sicherzustellen, dass kein bekanntes Virtual Private Network (VPN) oder Proxy-Service genutzt wird;
- c) Geräte zu erkennen und zu blockieren, die auf Manipulationen auf Systemebene hindeuten (z. B. Rooting, Jailbreaking etc.);

- d) „Man-In-The-Middle“-Angriffe oder ähnliche Hacking-Techniken zu stoppen und Code-Manipulationen zu verhindern; und
- e) auf Anwendungsebene verifizierbare Erkennungs- und Blockade-Mechanismen zu nutzen.

2.7.3 Standorterkennung in einem privaten Netzwerk

Wenn interaktives Spielen über ein privates Netzwerk wie ein Wireless Local Area Network (WLAN) erfolgt, muss das interaktive Spielsystem eine der folgenden Methoden beinhalten, um die Standorte aller mit dem Netzwerk verbundenen Spieler zu überwachen:

- a) Ein Dienst oder eine Anwendung zur Standorterkennung, wobei jeder Spieler vor der Initiierung jedes Spiels eine Standortprüfung durchlaufen muss. Dieser Service bzw. diese Anwendung muss die Anforderungen im nächsten Abschnitt zur „Standorterkennung in einem öffentlichen Netzwerk“ erfüllen; oder
- b) eine Komponente zur Standorterkennung, die in Echtzeit erkennt, wann sich jegliche Spieler nicht mehr innerhalb der zulässigen Grenzen befinden und die Teilnahme an weiteren Spielen verhindert. Dies kann mithilfe spezieller IT-Hardware wie Richtantennen, Bluetooth-Sensoren oder anderer Methoden erreicht werden, die das unabhängige Prüflabor auf fallweiser Basis beurteilt.

2.7.4 Standorterkennung in einem öffentlichen Netzwerk

Wenn interaktive Spiele in einem öffentlichen Netzwerk wie dem Internet stattfinden, muss das interaktive Spielsystem einen Dienst oder eine Anwendung zur Standorterkennung beinhalten, um den Standort eines Spielers, der versucht, an einem Spiel teilzunehmen, angemessen zu erkennen und dynamisch zu überwachen sowie das Blockieren nicht autorisierter Versuche zur Spielteilnahme zu überwachen und zu ermöglichen, diese Versuche zu verhindern.

- a) Jeder Spieler muss vor der Initiierung des ersten Spiels nach der Anmeldung über ein bestimmtes Remote-Spieler-Gerät eine Standortprüfung durchlaufen. Anschließende Standortprüfungen auf diesem Gerät müssen vor der Initiierung eines Spiels durchgeführt werden, nachdem eine Änderung der IP-Adresse des Spielers erkannt wurde, nachdem ein Zeitraum von dreißig Minuten seit der vorherigen Standortprüfung verstrichen ist oder nach sonstigen von der Regulierungsbehörde festgelegten Kriterien:
 - i. Wenn die Standortprüfung ergibt, dass sich der Spieler außerhalb der zulässigen Grenzen befindet, oder wenn der Standort des Spielers nicht erfolgreich ermittelt werden konnte, darf das Spiel nicht initiiert werden und der Spieler muss hierüber informiert werden.
 - ii. Bei jeder erkannten Standortverletzung muss ein Eintrag in einem zeitstempelfähigen Protokoll erstellt werden, der die eindeutige Spieler-ID sowie den erkannten Standort enthält.
- b) Es muss ein Verfahren zur Geolokalisierung eingesetzt werden, das Informationen zum physischen Standort eines Spielers sowie einen zugehörigen Konfidenzradius liefert. Der Konfidenzradius muss sich innerhalb der zulässigen Grenzen befinden.
- c) Genaue Standort-Datenquellen (Wi-Fi, GSM, GPS etc.) müssen von der Methode zur Geolokalisierung genutzt werden, um den Standort des Spielers zu bestätigen. Wenn es sich bei der einzigen Standort-Datenquelle eines Remote-Spieler-Geräts um eine IP-Adresse handelt,

können die Standortdaten eines für das Spielerkonto registrierten Mobilgeräts unter folgenden Bedingungen als unterstützende Standort-Datenquelle genutzt werden:

- i. Das Remote-Spieler-Gerät (auf dem das Spiel gespielt wird) und das Mobilgerät müssen sich in räumlicher Nähe zueinander befinden.
 - ii. Wenn von der Regulierungsbehörde gestattet, können Standortdaten des Netzbetreibers eines Mobilgeräts genutzt werden, sollten keine anderen Datenquellen außer IP-Adressen verfügbar sein.
- d) Das Verfahren zur Geolokalisierung muss kontrollieren können, ob der Genauigkeitsradius der Standort-Datenquelle definierte Pufferzonen oder die zulässigen Grenzen überschreiten darf.
- e) Zur Minderung und Berücksichtigung von Diskrepanzen zwischen Kartierungsquellen und Varianzen in raumbezogenen Daten sind von der Regulierungsbehörde genehmigte Grenzpolygone sowie Overlay-Standortdaten auf diesen Grenzpolygonen zu nutzen.
- f) Das Verfahren zur Geolokalisierung muss alle Spiele überwachen und für eine Untersuchung markieren, die über ein ein Einzelspielerkonto mit inkonsistenten Standorten gespielt werden (z. B. beim Spielen an aufeinanderfolgenden Standorten, die innerhalb der gemeldeten Zeitspanne nicht hätten besucht werden können).

2.8 Aufzubewahrende Informationen

2.8.1 Datenspeicherung und Zeitstempel

Das interaktive Spielsystem muss in der Lage sein, alle aufgezeichneten Daten zu speichern und zu sichern, wie in diesem Abschnitt dargelegt:

- a) Für alle Zeitstempel muss die Systemuhr verwendet werden.
- b) Das System muss einen Mechanismus bieten, um die Daten für Analyse- und Audit-/Verifizierungszwecke zu exportieren (z. B. CSV, XLS).

2.8.2 Spielinformationen

Für jedes einzelne von dem Spieler gespielte Spiel müssen die durch das interaktive Spielsystem zu speichernden und zu sichernden Informationen Folgendes beinhalten, sofern anwendbar:

- a) das Datum und die Uhrzeit, zu der das Spiel gespielt wurde;
- b) die für das Spiel gespielte Stückelung, sofern es sich um einen Spieltyp mit Mehrfach-Stückelung handelt;
- c) die mit dem Endergebnis des Spiels verbundene Anzeige, entweder grafisch oder mit einer klaren Textbeschreibung;
- d) die zu Beginn und/oder am Ende des Spiels als Einsatz verfügbaren Geldbeträge;
- e) den eingesetzten Gesamtbetrag, einschließlich jeglicher Anreizgutschriften;
- f) den gewonnenen Gesamtbetrag, einschließlich:
 - i. jeglicher Anreizgutschriften und/oder Preise; und
 - ii. alle progressiven Jackpots oder stufenweisen Jackpots;
- g) alle nicht einsatzbezogenen Käufe zwischen dem Beginn und dem Ende des Spiels;
- h) in Rechnung gestellte Rakes, Provisionen oder Gebühren;
- i) die Ergebnisse aller anderen am Spielergebnis beteiligten Spielerentscheidungen;

- j) die Ergebnisse aller Übergangs-Spielphasen wie Verdopplungs-/Risiko- oder Bonus-/Feature-Spiele;
- k) wenn ein progressiver Jackpot oder ein stufenweiser Jackpot gewonnen wurde, ein Hinweis, dass der Jackpot vergeben wurde;
- l) alle Ratschläge zum Spiel, die dem Spieler für Spiele mit Fähigkeitselementen angeboten wurden;
- m) alle progressiven Jackpots oder stufenweisen Jackpots;
- n) relevante Standortinformationen;
- o) der aktuelle Status des Spiels (laufend, abgeschlossen, unterbrochen, abgebrochen etc.);
- p) eindeutige Spielzyklus-ID und/oder Spielsitzungs-ID (sofern unterschiedlich);
- q) eindeutige Spielthemen-/Gewinntabellen-ID; und
- r) eindeutige Spieler-ID.

HINWEIS: Bei einzelnen Spielen mit mehreren Spielern müssen diese Informationen für jeden Spieler aufgezeichnet werden.

2.8.3 Spielthemen-/Gewinntabellen-Informationen

Für alle einzelnen für das Spiel verfügbaren Spielthemen und Gewinntabellen müssen die vom interaktiven Spielsystem erfassten und gesicherten Informationen Folgendes beinhalten, sofern anwendbar:

- a) eindeutige Spielthemen-/Gewinntabellen-ID;
- b) Spielkonfigurationsdaten (z. B. Stückelungen, Einsatzkategorien etc.);
- c) das Datum und die Uhrzeit, zu der das Spielthema/die Gewinntabelle für das Spiel zur Verfügung gestellt wurde;
- d) theoretische Ausschüttungsquote (RTP);
- e) die Anzahl der gespielten Spiele;
- f) Gesamtwert aller Einsätze, ohne:
 - i. jegliche eingesetzten Anreizgutschriften; und
 - ii. nachfolgende Einsätze von Zwischengewinnen, die während des Spiels erzielt wurden, beispielsweise aus Verdopplungs-/Risiko-Features;
- g) Gesamtwert der mit den Einsätzen erzielten Gewinne, ohne:
 - i. jegliche Anreizgutschriften und/oder gewonnenen Preise; und
 - ii. alle gewonnenen progressiven Jackpots und/oder stufenweisen Jackpots;
- h) Gesamtwert der Auszahlung von Gewinnen aus progressiven Jackpots und/oder inkrementellen Jackpots;
- i) Gesamtbetrag der eingesetzten Anreizgutschriften;
- j) Gesamtbetrag der Anreizgutschriften und/oder gewonnenen Preise;
- k) Gesamtbetrag aller ungültigen oder stornierten Einsätze, einschließlich jeglicher Anreizgutschriften;
- l) Gesamtbetrag aller nicht einsatzbezogenen Käufe in Verbindung mit dem Spiel;
- m) die Häufigkeit, mit der jeder Jackpot vergeben wurde;
- n) bei Spielen, die Verdopplungs-/Risiko-Features unterstützen:
 - i. für Verdopplungen/Risikospiele eingesetzter Gesamtbetrag;
 - ii. bei Verdopplungen/Risikospiele gewonnener Gesamtbetrag;
 - iii. Anzahl der gespielten Verdopplungs-/Risikospiele;

- iv. Anzahl der gewonnenen Verdopplungs-/Risikospiele;
- o) insgesamt in Rechnung gestellte Rakes, Provisionen oder Gebühren;
- p) der aktuelle Status des Spielthemas/der Gewinntabelle (aktiv, deaktiviert, außer Kraft gesetzt etc.); und
- q) das Datum und die Uhrzeit, zu der das Spielthema/die Gewinntabelle außer Kraft gesetzt werden sollte oder soll.

2.8.4 Wettbewerbs-/Turnier-Informationen

Bei interaktiven Spielsystemen, die Wettbewerbe/Turniere unterstützen, müssen die durch das interaktive Spielsystem zu speichernden und zu sichernden Informationen für jeden Wettbewerb/jedes Turnier Folgendes beinhalten, sofern anwendbar:

- a) Name oder Kennung des Wettbewerbs/Turniers;
- b) das Datum und die Uhrzeit, zu der der Wettbewerb/das Turnier stattfand oder stattfinden wird (sofern bekannt);
- c) ID(s) der teilnehmenden Spielthemen/Gewinntabellen;
- d) für jeden registrierten Spieler:
 - i. eindeutige Spieler-ID;
 - ii. Betrag der in Rechnung gestellten Teilnahmegebühren, einschließlich aller Anreizgutschriften und des Berechnungsdatums;
 - iii. Spieler-Punktzahlen/Ranglistenpositionen;
 - iv. Betrag der ausgezahlten Gewinne, einschließlich aller Anreizgutschriften und des Auszahlungsdatums;
- e) Betrag der in Rechnung gestellten Teilnahmegebühren, einschließlich aller Anreizgutschriften;
- f) Gesamt- Betrag der an die Spieler ausgezahlten Gewinne, einschließlich Anreizgutschriften;
- g) insgesamt in Rechnung gestellte Rakes, Provisionen oder Gebühren; und
- h) der aktuelle Status des Wettbewerbs/Turniers (laufend, abgeschlossen, unterbrochen, abgebrochen etc.).

2.8.5 Spielerkonto-Informationen

Für jedes Spielerkonto müssen die durch das interaktive Spielsystem zu speichernden und zu sichernden Informationen Folgendes beinhalten:

- a) eindeutige Spieler-ID und Benutzername (sofern unterschiedlich);
- b) personenbezogene Daten (PII) des Spielers, z. B.:
 - i. die Informationen, die vom Betreiber zur Registrierung eines Spielers und zur Erstellung des Kontos erfassten Informationen, einschließlich des offiziellen Namens, der Wohnanschrift und des Geburtsdatums;
 - ii. Verschlüsselte PII, einschließlich der behördlichen Identifikationsnummer (Sozialversicherungsnummern, Steuer-ID, Passnummer oder Vergleichbares), Authentifizierungsdaten (Passwort, PIN etc.) sowie persönliche Finanzinformationen (Debit-Instrumenten-Nummern, Kreditkarten-Nummern, Bankkonto-Nummern etc.);
- c) Datum und Methode der Identitätsprüfung, einschließlich, wo anwendbar, einer Beschreibung der von einem Spieler bereitgestellten Identifizierungsdaten zur Bestätigung der Identität sowie

- des Gültigkeitsdatums;
- d) das Datum, an dem der Spieler den Geschäftsbedingungen sowie der Datenschutzrichtlinie des Betreibers zugestimmt hat;
 - e) Kontodetails und aktueller Kontostand, einschließlich jeglicher Anreizgutschriften. Alle eingeschränkten Anreizgutschriften mit einem möglichen Gültigkeitsdatum müssen separat verwaltet werden;
 - f) vorherige Konten, sofern vorhanden, und Grund für deren Deaktivierung;
 - g) das Datum und die Methode der Kontoregistrierung (z. B. remote oder vor Ort);
 - h) das Datum und die Uhrzeit des Kontozugriffs durch beliebige Personen (Spieler oder Betreiber), einschließlich IP-Adresse;
 - i) Informationen zu Ausschlüssen/Einschränkungen, wie von der Regulierungsbehörde gefordert:
 - i. Datum und Uhrzeit der Aufforderung (sofern anwendbar);
 - ii. Beschreibung und Grund des Ausschlusses/der Einschränkung;
 - iii. Art des Ausschlusses/der Einschränkung (z. B. durch den Betreiber verhängter Ausschluss, selbstgewählte Einzahlungsbeschränkung);
 - iv. Datum des Beginns des Ausschlusses/der Einschränkung;
 - v. Datum des Endes des Ausschlusses/der Einschränkung (sofern anwendbar);
 - j) Informationen zu Finanztransaktionen:
 - i. Art der Transaktion (z. B. Einzahlung, Auszahlung, Anpassung, nicht einsatzbezogener Kauf);
 - ii. Datum und Uhrzeit der Transaktion;
 - iii. Eindeutige Transaktions-ID;
 - iv. Transaktionsbetrag;
 - v. Gesamtkontostand vor/nach der Transaktion;
 - vi. Gesamtbetrag der für die Transaktion gezahlten Gebühren (sofern zutreffend);
 - vii. Kennung des Benutzers, der die Transaktion abgewickelt hat (sofern anwendbar);
 - viii. Transaktionsstatus (ausstehend, abgeschlossen etc.);
 - ix. Einzahlungs-/Auszahlungsmethode (z. B. Bargeld, Barscheck, Bankscheck, Überweisung, Postanweisung, Lastschriftinstrument, Kreditkarte, elektronischer Zahlungsverkehr etc.);
 - x. Einzahlungs-Autorisierungsnummer;
 - xi. relevante Standortinformationen.
 - k) Persistenz-Spielinformationen, sofern vom interaktiven Spielsystem unterstützt:
 - i. Eindeutige Spielthemen-/Gewinntabellen-ID, sofern an ein bestimmtes Spielthema oder eine bestimmte Gewinntabelle gebunden;
 - ii. Spielerfolge, erworbene Fähigkeiten oder ähnliches;
 - iii. letzter Speicherpunkt, wenn gespeicherte Spiele unterstützt werden;
 - l) Kennungsinformationen, sofern vom interaktiven Spielsystem unterstützt:
 - i. Eindeutige Spielthemen-/Gewinntabellen-ID, sofern an ein bestimmtes Spielthema oder eine bestimmte Gewinntabelle gebunden;
 - ii. Datum und Uhrzeit der Transaktion;
 - iii. eindeutige Transaktions-ID;
 - iv. die Kriterien für die Nutzung der Kennung (Fähigkeitsniveau, Abonnements, Kontomitgliedschaften, Spieler-Tracking-Informationen, Fähigkeitsanforderungen des Spiels etc.);
 - v. Art der ergriffenen Maßnahme oder am Spiel vorgenommenen Änderung (z. B. Änderung der Spielregeln, Änderung der Gewinntabelle oder andere Konfigurationsänderungen in Verbindung mit dem Spielergebnis); und

m) aktueller Status des Spielerkontos (z. B. aktiv, inaktiv, geschlossen, ausgeschlossen etc.).

2.8.6 Anreiz-Informationen

Bei interaktiven Spielsystemen, die Anreizprämien unterstützen, welche gegen Geld, Einsatzguthaben oder Merchandise-Artikel eingelöst werden können, müssen die durch das interaktive Spielsystem zu speichernden und zu sichernden Informationen für jeden angebotenen Anreiz Folgendes beinhalten, sofern anwendbar:

- a) eindeutige ID des Anreizangebots;
- b) Datum und Uhrzeit, zu welcher der Anreiz zur Verfügung gestellt wurde;
- c) aktueller Kontostand für Anreizprämien;
- d) Gesamtbetrag der ausgegebenen Anreizprämien;
- e) Gesamtbetrag der eingelösten Anreizprämien;
- f) Gesamtbetrag der Anreizprämien mit abgelaufener Gültigkeit;
- g) Gesamtbetrag der Anreizprämien-Anpassungen;
- h) der aktuelle Status des Anreizes (aktiv, deaktiviert, außer Kraft gesetzt etc.); und
- i) Datum und Uhrzeit, zu der der Anreiz außer Kraft gesetzt wurde oder außer Kraft gesetzt werden soll (leer bis bekannt).

2.8.7 Jackpot-Informationen

Bei interaktiven Spielsystemen, die progressive Jackpots oder stufenweise Jackpots unterstützen, müssen die durch das interaktive Spielsystem für jeden angebotenen Jackpot zu speichernden und zu sichernden Informationen Folgendes beinhalten, sofern anwendbar:

- a) eindeutige Jackpot-ID (sofern der Jackpot nicht an ein bestimmtes Spielthema, eine bestimmte Gewinntabelle oder einen bestimmten Spieler gebunden ist);
- b) Datum und Uhrzeit, zu welcher der Jackpot zur Verfügung gestellt wurde;
- c) ID(s) der teilnehmenden Spielthemen/Gewinntabellen;
- d) eindeutige Spieler-ID(s), wenn der Jackpot an bestimmte Spieler gebunden ist;
- e) aktueller Wert des Jackpots (Auszahlung);
- f) jegliche anderen Pools mit Jackpot-Beiträgen, sofern anwendbar:
 - i. aktueller, die Deckelung übersteigender Wert, wo von der Regulierungsbehörde gefordert (Überlauf);
 - ii. aktueller Wert des Jackpot-Umleitungs-Schemas (Umleitungspool);
- g) Resetwert des aktuellen Jackpots, sofern abweichend vom Startwert (Resetwert);
- h) wenn solche Parameter nach der ersten Einrichtung konfigurierbar sind:
 - i. Anfangswert des Jackpots (Startwert);
 - ii. anteilige Erhöhungsrates (Inkrement);
 - iii. Jackpot-Grenzwert (Deckelung);
 - iv. anteilige Erhöhungsrates nach Erreichen der Deckelung (sekundäres Inkrement);
 - v. anteilige Erhöhungsrates für Umleitungspool (verborgenes Inkrement);
 - vi. Umleitungspool-Grenzwert (Umleitungslimit);
 - vii. die Wahrscheinlichkeiten für das Auslösen des Jackpots (Wahrscheinlichkeiten);
 - viii. alle Parameter, die Zeiträume angeben, in denen der Jackpot ausgelöst werden kann

- (Zeitlimit);
- ix. alle zusätzlichen Informationen, die zum Abgleich des Jackpots benötigt werden;
 - i) der aktuelle Status des Jackpots (aktiv, deaktiviert, außer Kraft gesetzt etc.); und
 - j) Datum und Uhrzeit, zu der der Jackpot außer Kraft gesetzt wurde oder außer Kraft gesetzt werden soll (leer bis bekannt).

HINWEIS: Es wird erwartet, dass dem Betreiber für nicht konfigurierbare Parametern, die nicht vom interaktiven Spielsystem gespeichert oder gesichert werden, Dokumentationen zur Verfügung stehen, die diese statischen Werte enthalten.

2.8.8 Informationen über signifikante Ereignisse

Informationen über signifikante Ereignisse, die durch das interaktive Spielsystem zu speichern und zu sichern sind, müssen Folgendes enthalten, sofern anwendbar:

- a) fehlgeschlagene Kontozugriffs-Versuche, einschließlich IP-Adresse;
- b) Programmfehler oder nicht übereinstimmende Authentifizierungsdaten;
- c) signifikante Zeiträume ohne Verfügbarkeit jeglicher kritischen Komponenten des Systems (jede Unterbrechung der Spieldauer für alle Spieler und/oder Transaktionen, die für beliebige Benutzer nicht erfolgreich durchgeführt werden können);
- d) hohe Gewinne (einzelne und während des definierten Zeitraums aufgelaufene), die einen von der Regulierungsbehörde festgelegten Wert überschreiten, einschließlich Spielinformationen;
- e) hohe Einsätze (einzelne und während des definierten Zeitraums aufgelaufene), die einen von der Regulierungsbehörde festgelegten Wert überschreiten, einschließlich Spielinformationen;
- f) Systemfehler, Außerkraftsetzungen und Korrekturen;
- g) Änderungen an Live-Datendateien außerhalb der normalen Programm- und Systemausführung;
- h) Änderungen an der Download-Datenbibliothek, einschließlich Hinzufügens, Ändern oder Löschens von Software, wo unterstützt;
- i) Änderungen an Richtlinien und Parametern für Betriebssysteme, Datenbanken, Netzwerke und Anwendungen (z. B. Audit-Einstellungen, Einstellungen der Passwort-Komplexität, Systemsicherheits-Niveaus, manuelle Aktualisierungen von Datenbanken etc.);
- j) Änderungen am Datum/der Uhrzeit des Master-Zeitservers;
- k) Änderungen an den Spielthemen-Parametern (z. B. Spielregeln, Auszahlungspläne, Rake-Anteil, Gewinntabellen etc.);
- l) Änderungen an den Parametern für progressive Jackpots oder stufenweise Jackpots;
- m) Änderungen an Anreizparametern (z. B. Beginn/Ende, Wert, Anspruch, Einschränkungen etc.);
- n) Spielerkontenverwaltung:
 - i. Anpassungen an einem Spielerkontostand;
 - ii. Änderungen an PII und anderen sensiblen Informationen, die in einem Spielerkonto gespeichert sind;
 - iii. Deaktivierung eines Spielerkontos;
 - iv. große Finanztransaktionen (einzelne und während des definierten Zeitraums aufgelaufene), die einen von der Regulierungsbehörde festgelegten Wert überschreiten, einschließlich Transaktionsinformationen;
 - v. negativer Spielerkontostand (aufgrund von Anpassungen und/oder Rückbuchungen);
- o) unwiederbringlicher Verlust von PII und anderen sensiblen Informationen;

- p) alle anderen Aktivitäten, die ein Eingreifen durch den Benutzer erfordern und außerhalb des normalen Systembetriebs erfolgen; und
- q) andere signifikante oder ungewöhnliche Ereignisse, die von der Regulierungsbehörde als anwendbar angesehen werden.

2.8.9 Informationen zum Benutzerzugriff

Für jedes Benutzerkonto müssen die durch das interaktive Spielsystem zu speichernden und zu sichernden Informationen Folgendes beinhalten:

- a) Mitarbeitername sowie Titel oder Position;
- b) Benutzerkennung;
- c) vollständige Liste und Beschreibung der Funktionen, die von jeder Gruppe oder jedem Benutzerkonto ausgeführt werden können;
- d) Datum und Uhrzeit der Kontoerstellung;
- e) Datum und Uhrzeit des letzten Zugriffs, einschließlich IP-Adresse;
- f) Datum und Uhrzeit der letzten Passwortänderung;
- g) Datum und Uhrzeit der Deaktivierung des Kontos;
- h) Gruppenzugehörigkeit des Benutzerkontos (sofern anwendbar); und
- i) aktueller Status des Benutzerkontos (z. B. aktiv, inaktiv, geschlossen, vorübergehend gesperrt etc.).

2.9 Berichtsansforderungen

2.9.1 Allgemeine Berichtsansforderungen

Das interaktive Spielsystem muss in der Lage sein, die Informationen zu generieren, die zur Erstellung der von der Regulierungsbehörde geforderten Berichte benötigt werden. Über die Anforderungen im obigen Abschnitt „Datenspeicherung und Zeitstempel“ hinaus gelten die folgenden Anforderungen für die erforderlichen Berichte:

- a) Das System muss in der Lage sein, die Berichtsinformationen auf Abruf täglich sowie in anderen von der Regulierungsbehörde verlangten Intervallen bereitzustellen (z. B. Vormonat, Vorjahr, Gesamt etc.).
- b) Jeder erforderliche Bericht muss Folgendes beinhalten:
 - i. den Namen des Betreibers (oder eine andere Bezeichnung), den Titel des Berichts, das ausgewählte Intervall sowie das Datum/die Uhrzeit der Berichtserstellung;
 - ii. einen Hinweis auf „keine Aktivität“ oder eine vergleichbare Meldung, wenn für den angegebenen Zeitraum keine Informationen vorliegen; und
 - iii. gekennzeichnete Bereiche, die entsprechend ihrer Funktion klar verstanden werden können.

HINWEIS: Neben den in diesem Abschnitt genannten Berichten kann die Regulierungsbehörde ebenfalls andere Berichte verlangen, welche die gemäß Abschnitt „Zu speichernde Informationen“ dieses Dokuments zu speichernden Daten nutzen.

2.9.2 Berichte zur Spiel-Leistung

Das interaktive Spielsystem muss in der Lage sein, die folgenden Informationen bereitzustellen, die zur Erstellung eines oder mehrerer Berichte zur Spiel-Leistung für jedes Spielthema oder jede Gewinnntabelle benötigt werden:

- a) den Namen des Spielthemas und den Spieltyp (Automat, Blackjack, Poker, Tisch etc.);
- b) das Datum und die Uhrzeit, zu der das Spielthema/die Gewinnntabelle für das Spiel zur Verfügung gestellt wurde;
- c) bei Hausbank-Spielen:
 - i. theoretische Ausschüttungsquote;
 - ii. aktuelle Ausschüttungsquote;
- d) die Anzahl der gespielten Spiele;
- e) Gesamtbetrag aller Einsätze, einschließlich separater Beträge für Anreizgutschriften;
- f) Gesamtbetrag der an die Spieler ausgezahlten Gewinne, einschließlich separater Beträge für Anreizgutschriften und/oder Preise;
- g) Gesamtbetrag aller ungültigen oder stornierten Einsätze, einschließlich separater Beträge für Anreizgutschriften;
- h) insgesamt in Rechnung gestellte Rakes, Provisionen oder Gebühren;
- i) Gesamtbetrag aller in unterbrochenen Spielen verbleibenden Gelder, einschließlich separater Beträge für Anreizgutschriften;
- j) Spiel Themen-/Gewinntabellen-ID; und
- k) der aktuelle Status des Spielthemas/der Gewinnntabelle (aktiv, deaktiviert, außer Kraft gesetzt etc.).

2.9.3 Berichte zur Betreiberhaftung

Das interaktive Spielsystem muss in der Lage sein, die folgenden Informationen bereitzustellen, die zur Erstellung eines oder mehrerer Berichte zur Betreiberhaftung benötigt werden, sofern anwendbar:

- a) Gesamtbetrag, den der Betreiber für die Spielerkonten verwaltet; und
- b) jegliche Betriebsmittel zur Deckung jeder sonstigen Betreiberhaftung, sofern durch die Regulierungsbehörde definiert.

2.9.4 Berichte zu großen Jackpot-Auszahlungen

Bei interaktiven Spielsystemen, die progressive oder stufenweise Jackpots unterstützen, muss das interaktive Spielsystem in der Lage sein, die folgenden Informationen bereitzustellen, die zur Erstellung eines oder mehrerer Berichte zu Jackpot-Auszahlungen oberhalb eines bestimmten, von der Regulierungsbehörde definierten Werts erforderlich sind, sofern anwendbar:

- a) eindeutige Jackpot-ID (sofern der Jackpot nicht an ein bestimmtes Spielthema, eine bestimmte Gewinnntabelle oder einen bestimmten Spieler gebunden ist);
- b) ID des gewinnenden Spielers;
- c) Gewinn-Spielthemen-/Gewinntabellen-ID;

- d) Gewinn-Spielzyklus-ID und/oder Spielsitzungs-ID (sofern unterschiedlich);
- e) Datum und Uhrzeit der Jackpot-Auslösung;
- f) Jackpot-Gewinn- und Auszahlungsbetrag; und
- g) Kennung der Benutzer, die den Gewinn erzielt und/oder bestätigt haben.

2.9.5 Berichte über signifikante Ereignisse und Änderungen

Das interaktive Spielsystem muss in der Lage sein, die folgenden Informationen bereitzustellen, die zur Erstellung eines oder mehrerer Berichte zu signifikanten Ereignissen oder Änderungen benötigt werden, sofern anwendbar:

- a) Datum und Uhrzeit des signifikanten Ereignisses oder der signifikanten Änderung;
- b) Ereignis-/Komponentenbezeichnung;
- c) Kennung der Benutzer, die das signifikante Ereignis oder die signifikante Änderung bewirkt und/oder autorisiert haben;
- d) Grund/Beschreibung des signifikanten Ereignisses oder der signifikanten Änderung, einschließlich geänderter Daten oder Parameter;
- e) Daten- oder Parameterwert vor der Änderung; und
- f) Daten- oder Parameterwert nach der Änderung.

Anforderungen an Zufallszahlengenerator (RNG)

3.1 Einleitung

3.1.1 Allgemeines

In diesem Kapitel werden die technischen Anforderungen für einen Zufallszahlengenerator (RNG) dargelegt. Die Arten von RNGs umfassen die Folgenden:

- a) Software-basierte RNGs nutzen keine Hardware-Geräte und leiten ihre Zufälligkeit grundsätzlich und primär aus einem computer-basierten oder software-gestützten Algorithmus ab. Sie beinhalten keinerlei Hardware-Zufälligkeit, gleich welcher Art.
- b) Hardware-basierte RNGs leiten ihre Zufälligkeit aus kleinen physischen Ereignissen ab (z. B. Stromkreis-Rückwirkung, thermisches Rauschen, radioaktiver Zerfall, Photonen-Spin etc.).
- c) Mechanische RNGs generieren Spielergebnisse mechanisch mithilfe physikalischer Gesetze (z. B. Kessel, Trommeln, Gebläse, Mischer etc.).

HINWEIS: Bitte beachten Sie ebenfalls die Anforderungen im Abschnitt „Spielergebnis mithilfe eines Zufallszahlengenerators“ des Kapitels „Spielanforderungen“ dieser Norm.

3.2 Allgemeine RNG-Anforderungen

3.2.1 Quellcode-Prüfung

Das unabhängige Prüflabor muss den zu jedem beliebigen Kern-Zufallsalgorithmus, Skalierungsalgorithmus, Mischalgorithmus und zu anderen Algorithmen oder Funktionen gehörenden Quellcode prüfen, die von entscheidender Bedeutung für das endgültige Zufallsergebnis eines Spiels sind. Diese Prüfung muss einen Vergleich mit veröffentlichten Referenzen beinhalten, wo anwendbar, sowie eine Untersuchung in Bezug auf Voreingenommenheit, Implementierungsfehler, schädlichen Code, Code mit dem Potenzial zur Verhaltensmanipulation oder unbekannte Umstellungen oder Parameter mit einem möglichen Einfluss auf die Zufälligkeit und ein faires Spiel.

3.2.2 Statistische Analyse

Das unabhängige Prüflabor nutzt statistische Prüfungen zur Bewertung der vom RNG erzeugten Ergebnisse nach dem Skalieren, Mischen oder anderen Zuordnungen (nachfolgend als „Endergebnis“ bezeichnet). Das unabhängige Prüflabor muss von Fall zu Fall jeweils geeignete Tests auswählen, abhängig vom geprüften RNG sowie dessen Nutzung innerhalb des Spiels. Die Tests müssen ausgewählt werden, um eine Konformität mit der beabsichtigten Werteverteilung, statistischen Unabhängigkeit einzelner Ziehungen sowie, falls anwendbar, statistischen Unabhängigkeit mehrerer Werte innerhalb einer einzelnen Ziehung sicherzustellen. Die angewendeten Tests müssen gemeinsam mit einem Konfidenzniveau von 99 % beurteilt werden. Die Menge an Testdaten muss so gewählt sein, dass signifikante Abweichungen von den anwendbaren RNG-Prüfkriterien mit hoher Frequenz erkannt werden. Falls ein RNG für eine variable Nutzung vorgesehen ist, liegt es in der

Verantwortung des unabhängigen Prüflabors, eine repräsentative Auswahl von Anwendungsfällen für die Prüfungen auszuwählen. Statistische Prüfungen können eine oder mehrere der folgenden Prüfungen enthalten:

- a) Gesamtverteilungs- oder Chi-Quadrat-Test;
- b) Überlappungstest;
- c) Gutscheinsammlertest;
- d) Starttest;
- e) Zusammenspiel-Korrelationstest;
- f) serieller Korrelationstest; und
- g) Duplikat-Test.

3.2.3 Verteilung

Jede mögliche RNG-Auswahl muss die gleiche Auswahlwahrscheinlichkeit aufweisen. Wo die Spielgestaltung eine nicht einheitliche Verteilung vorgibt, muss das Endergebnis der beabsichtigten Verteilung entsprechen.

- a) Alle verwendeten Skalierungs-, Kartierungs- und Mischalgorithmen müssen erwartungstreu sein, was durch die Quellcode-Prüfung zu bestätigen ist. Das Verwerfen von RNG-Werten ist in diesem Zusammenhang zulässig und kann notwendig sein, um eine Tendenz zu beseitigen.
- b) Das Endergebnis muss hinsichtlich der beabsichtigten Verteilung mithilfe geeigneter statistischer Tests (z. B. Gesamtverteilungstest) überprüft werden.

3.2.4 Unabhängigkeit

Die Kenntnis der in einer Ziehung ausgewählten Zahlen darf keine Informationen zu den möglicherweise in einer zukünftigen Ziehung ausgewählten Zahlen beinhalten. Wenn der RNG mehrere Zahlen im Zusammenhang mit einer einzelnen Ziehung auswählt, darf die Kenntnis eines oder mehrerer Werte keine Informationen über andere Werte innerhalb der Ziehung liefern, sofern dies nicht durch den Spielaufbau vorgesehen ist.

- a) Gemäß Verifizierung im Rahmen der Quellcode-Prüfung darf der RNG keine Auswahlen verwerfen oder modifizieren, die auf vorherigen Auswahlen basieren, sofern dies nicht durch den Spielaufbau vorgesehen ist (z. B. Ersatzlos-Funktion).
- b) Das Endergebnis muss mithilfe statistischer Tests auf Unabhängigkeit hinsichtlich anderer Ziehungen und, sofern anwendbar, Unabhängigkeit in Bezug auf eine Ziehung geprüft werden (z. B. serielle oder Zusammenspiel-Korrelationstests und Starttests).

3.2.5 Verfügbare Ergebnisse

Gemäß Verifizierung im Rahmen der Quellcode-Prüfung müssen die von der RNG-Lösung erzeugten möglichen Ergebnisse (d. h. der RNG-Zeitraum) insgesamt eine ausreichende Größe aufweisen, um sicherzustellen, dass alle Ergebnisse für jede Ziehung mit der angemessenen Wahrscheinlichkeit verfügbar sind, unabhängig von vorherigen Ergebnissen, sofern dies nicht durch den Spielaufbau vorgegeben ist.

3.3 RNG-Stärke und -Überwachung

3.3.1 RNG-Stärke zur Ergebnisfestlegung

Der bei der Festlegung der Spielergebnisse innerhalb einer Gaming-Plattform verwendete RNG muss kryptographisch stark sein. „Kryptographisch stark“ bedeutet, dass der RNG widerstandsfähig gegen Angriffe oder Kompromittierungen durch einen intelligenten Angreifer mit modernen Computing-Ressourcen sowie möglicher Kenntnis des RNG-Quellcodes ist.

3.3.2 Kryptographische RNG-Angriffe

Ein kryptographischer RNG kann nicht problemlos durch einen erfahrenen Angreifer mit Kenntnis des Quellcodes kompromittiert werden. Mindestens müssen kryptographische RNGs widerstandsfähig gegen die folgenden Angriffsarten sein:

- a) direkter kryptographischer Angriff: Mithilfe in der Vergangenheit durch den RNG erzeugter Werte darf es rechnerisch nicht möglich sein, zukünftige RNG-Werte vorherzusagen oder zu schätzen. Dies muss durch die entsprechende Nutzung eines anerkannten kryptographischen Algorithmus (RNG-Algorithmus, Hash, Chiffre etc.) sichergestellt werden. Es ist zu beachten, dass hardware-basierte RNGs oder mechanische RNGs potenziell als kryptografischer Algorithmus geeignet sein können, sofern sie die statistischen Tests bestehen;
- b) bekannte Eingabe-Angriffe: Es muss unmöglich sein, den RNG-Status nach der ersten Initiierung rechnerisch zu bestimmen oder sinnvoll zu schätzen. Insbesondere darf der RNG nicht allein durch einen zeitgesteuerten Wert initiiert werden. Der Hersteller muss sicherstellen, dass die Spiele nicht dieselbe erste Initiierung nutzen. Die Initiierungsmethoden dürfen nicht die kryptographische Stärke des RNG beeinträchtigen; und
- c) State Compromise Extension-Angriffe: Der RNG muss mithilfe externer Entropie regelmäßig seinen Status modifizieren und die effektive Dauer jeglicher Ausnutzung potenzieller Schwachstellen durch einen erfolgreichen Hacker begrenzen.

HINWEIS: Durch kontinuierliche Verbesserungen und Fortschritte in der kryptographischen Forschung muss die Einhaltung dieses Kriteriums entsprechend den Anforderungen der Regulierungsbehörde neu beurteilt werden.

3.3.3 Dynamische Ergebnisüberwachung für hardware-basierte RNGs

Aufgrund ihrer physischen Natur kann sich die Leistung hardware-basierter RNGs im Laufe der Zeit unabhängig von der Spielplattform verschlechtern oder andere Fehlfunktionen aufweisen. Die Störung eines hardware-basierten RNG könnte ernsthafte Folgen für die vorgesehene Nutzung des RNG haben. Daher muss bei Einsatz eines hardware-basierten RNG eine dynamische Überwachung der Ergebnisse mithilfe statistischer Tests erfolgen. Dieser Überwachungsprozess muss den Spielablauf unterbrechen, wenn Fehlfunktionen oder Verschlechterungen festgestellt werden.

3.4 Mechanischer RNG (physisches Zufallsgerät)

3.4.1 Allgemeines

Die in diesem Abschnitt definierten Anforderungen gelten für mechanische RNGs oder „physische Zufallsgeräte“. Wenngleich die Software Bestandteil des Geräts sein kann, ist sie primär auf den Maschinenbetrieb und/oder das Lesen und Aufzeichnen von Spielergebnisdaten beschränkt (die Software spielt keine deterministische Rolle bei der Bestimmung des Spielergebnisses).

HINWEIS: Geräte, die präzise und mechanisch ein von einem Computer-RNG ausgewähltes Spielergebnis erzeugen oder anzeigen, werden nicht als physische Zufallsgeräte angesehen und müssen als RNG getestet werden, sobald eine genaue Reproduktion des vom RNG ausgewählten Ergebnisses sichergestellt ist. Physische Zufallsgeräte können RNGs in sekundärer Funktion beinhalten (z. B. Rotationsgeschwindigkeit). Solche sekundären RNGs müssen gemäß den in diesem Dokument enthaltenen RNG-Anforderungen beurteilt werden, da sie das Spielergebnis nicht direkt auswählen. Das physische Zufallsgerät sollte besser ganzheitlich getestet werden, wie in diesem Abschnitt beschrieben.

HINWEIS: Die zugelassenen Komponenten eines physischen Zufallsgeräts können nicht ausgelagert oder durch nicht zugelassene Komponenten ersetzt werden, da sie entscheidend für das Verhalten und die Leistung des physischen Zufallsgeräts sind. Die „zugelassenen Komponenten“ beinhalten in diesem Zusammenhang die physischen Elemente zur Erzeugung des zufälligen Verhaltens – z. B. Kugeln oder Karten in einem entsprechenden Mischgerät etc. Beispielsweise kann ein von dem unabhängigen Prüflabor zur Nutzung von Kunststoffkarten zertifiziertes Mischgerät nicht als zulässiges Äquivalent zum gleichen mechanischen Mischgerät für Papierkarten angesehen werden.

3.4.2 Datenerfassung

Für eine bestmögliche Garantie eines zufälligen Verhaltens muss das unabhängige Prüflabor die Daten von mindestens 10.000 Spielergebnissen erfassen. Die Datenerfassung muss auf eine angemessene Weise erfolgen, ähnlich der bestimmungsgemäßen Verwendung des Geräts in der Praxis. Insbesondere muss anfänglich die empfohlene Einrichtung und Kalibrierung erfolgen und die Gerätekomponenten (Karten, Kugeln etc.) müssen während des Erfassungszeitraums gemäß den Empfehlungen des Herstellers ausgetauscht oder instand gehalten werden.

HINWEIS: Aufgrund von Bedenken bezüglich der Machbarkeit in Verbindung mit einer angemessenen Datenerfassung auf manchen Geräten kann die Regulierungsbehörde im Einzelfall ebenfalls Testergebnisse akzeptieren, die mithilfe eines geringeren Datenvolumens gewonnen werden. Ebenso ist es möglich, dass ein größeres Datenvolumen erforderlich ist. Ungeachtet dessen wird das unabhängige Prüflabor in der anwendbaren Zertifizierung den Umfang der für die Tests genutzten Datenmenge klar angeben. Wenn weniger als 10.000 Spiele genutzt werden, ist dem Zertifizierungsbericht ein klarer Hinweis auf die statistischen Beschränkungen hinzuzufügen.

3.4.3 Langlebigkeit

Alle mechanischen Teile müssen aus Materialien bestehen, die eine Verschlechterung jeglicher Komponenten während der vorgesehenen Nutzungsdauer verhindern.

HINWEIS: Das unabhängige Prüflabor kann einen strengeren Austausch-Zeitplan empfehlen als der Hersteller des Geräts, um die obigen „Langlebigkeits“-Anforderungen zu erfüllen. Darüber hinaus kann das unabhängige

Prüflabor eine regelmäßige Inspektion des Geräts empfehlen, um dessen Integrität zu gewährleisten und aufrechtzuerhalten.

3.4.4 Manipulation

Die Spieler und/oder Spielbeteiligten (z. B. Kartengeber, Croupiers etc.) in Live-Spielen dürfen nicht über die Möglichkeit verfügen, die physischen Zufallsgeräte auf physische Art und Weise hinsichtlich der Erzeugung von Spielergebnisdaten zu manipulieren oder zu beeinflussen, sofern nicht durch den Spielbau vorgesehen.

Spielanforderungen

4.1 Einleitung

4.1.1 Allgemeines

In diesem Kapitel werden die technischen Anforderungen an die Spielerschnittstelle, die Spielregeln, Spiel-Fairness, Spielauswahl, Spielergebnis, zugehörige Spielanzeigen sowie Illustrationen, Auszahlungsraten und Quoten, Bonus-/Feature-Spiele, progressive Jackpots, stufenweise Jackpots, Spiel-Rückruf, Spielmodi, allgemeine Funktionen, Spiele mit Fähigkeitselementen und andere Spielanforderungen dargelegt.

HINWEIS: Bitte beachten Sie den Abschnitt „Spiele mit Fähigkeitselementen“ dieser technischen Norm für besondere und ergänzende Anforderungen an Spiele mit einem oder mehreren Fähigkeitselementen.

4.2 Spielerschnittstelle

4.2.1 Allgemeines

Die Spielerschnittstelle ist definiert als eine Schnittstellenanwendung oder ein Programm, über das der Benutzer Anzeigen der Spieler-Software erhält und mit dieser interagiert, einschließlich Touchscreen(s), Tastatur, Maus oder anderer Formen von Geräten zur Spielerinteraktion.

4.2.2 Anforderungen an die Spielerschnittstelle

Die Spielerschnittstelle muss die folgenden Anforderungen erfüllen:

- a) Bei jeglichen Größenänderungen oder Überlagerungen der Spielerschnittstelle müssen präzise Zuordnungen erfolgen, um den geänderten Anzeigebereich und Touch-/Klickpunkte korrekt widerzuspiegeln.
- b) Alle vom Spieler auswählbaren Touch-/Klickpunkte oder Schaltflächen, die auf der Spielerschnittstelle dargestellt sind und sich auf den Spielablauf und/oder die Integrität oder das Ergebnis des Spiels auswirken, müssen entsprechend ihrer Funktion klar gekennzeichnet sein und ihre Funktionsweise muss den anwendbaren Spielregeln entsprechen.
- c) An keiner Stelle der Spielerschnittstelle dürfen verborgene oder nicht dokumentierte Touch-/Klickpunkte oder Schaltflächen vorhanden sein, die sich auf den Spielablauf auswirken und/oder die Integrität oder das Ergebnis des Spiels beeinflussen, sofern nicht durch die Spielregeln vorgesehen.
- d) Die Anzeige von Anweisungen und Informationen muss an die Spielerschnittstelle angepasst werden. Wenn ein Gerät beispielsweise Technologien mit einer kleineren Bildschirmanzeige nutzt, ist es zulässig, eine gekürzte Version der Spielinformationen anzuzeigen, die direkt innerhalb des Spielbildschirms zugänglich ist, und die vollständige Version der Spielinformationen mithilfe einer anderen Methode, beispielsweise über einen zweiten Bildschirm, einen Hilfebildschirm oder eine andere Schnittstelle anzuzeigen, die auf dem optischen Spielbildschirm leicht erkennbar ist.

- e) Wo mehrere Anweisungs- und Informationselemente auf der Benutzerschnittstelle angezeigt werden, ist es akzeptabel, diese Informationen im Wechsel darzustellen, sofern die Wechselhäufigkeit der Informationen einem Spieler genügend Zeit zum Lesen aller Elemente bietet.

4.2.3 Gleichzeitige Eingaben

Die gleichzeitige oder aufeinanderfolgende Aktivierung verschiedener Geräte zur Spieler-Interaktion darf keine Fehlfunktionen des Spiels verursachen und nicht zu Ergebnissen führen, die dem beabsichtigten Spielaufbau widersprechen.

4.3 Spielsitzungs-Anforderungen

4.3.1 Allgemeines

Eine Spielsitzung ist definiert als Zeitraum, der mindestens beginnt, wenn ein Spieler ein Spiel oder eine Reihe von Spielen auf einer Spielplattform für ein bestimmtes Spielthema initiiert, indem er einen Einsatz platziert, und der endet, wenn ein Endergebnis für dieses Spiel oder die Reihe von Spielen vorliegt, wodurch der Spieler gleichzeitig die Möglichkeit erhält, das Spiel zu verlassen.

HINWEIS: Diese Norm soll keine Konzepte ausschließen oder verbieten, die das gleichzeitige Spielen mehrerer Spielthemen auf einer Spielplattform gestatten. Wenn mehrere Spielthemen gleichzeitig zugänglich sind, können die Spieler in separaten Spielsitzungen an mehr als einem Spiel gleichzeitig teilnehmen. Jedoch müssen in einem solchen Fall Messungen erfolgen und anwendbare Limits für jedes verfügbare Spiel durchgesetzt werden, wenn es gespielt wird, und alle anderen Anforderungen in diesem Kapitel müssen weiterhin für diese Konzepte mit mehreren gleichzeitigen Spielen gelten.

4.3.2 Spielauswahl

Die folgenden Anforderungen gelten für die Auswahl eines bestimmten Spiels auf der Spielerschnittstelle:

- a) Die Spielplattform muss den Spieler klar über alle zum Spielen verfügbaren Spiele informieren.
- b) Der Spieler muss darauf aufmerksam gemacht werden, welches Spielthema zum Spielen ausgewählt wurde und gespielt wird.
- c) Der Spieler darf nicht allein durch Auswählen eines Spielthemas zum Spielen eines Spiels gezwungen werden, sofern auf dem Spielbildschirm kein klarer Hinweis erfolgt, dass die Spielauswahl nicht geändert werden kann. Sofern nicht bekannt, muss der Spieler die Möglichkeit erhalten, zum Bildschirm des Hauptmenüs oder der Spielauswahl zurückzukehren.
- d) Die Standard-Spielanzeige beim Eintritt in den Spielmodus von einem Hauptmenü oder einer Bildschirmauswahl aus darf nicht der höchsten beworbenen Prämie entsprechen (sofern dies nicht das Ergebnis des letzten Spiels des Spielers war). Dies gilt nur für den primären Spielverlauf und nicht für sekundäre Boni/Features.

4.3.3 Spielanforderungen

Die folgenden Anforderungen gelten für das Spiel innerhalb einer Spielsitzung:

- a) Ein Spielzyklus besteht aus allen Spieleraktionen und Spielaktivitäten, die zwischen zwei Einsätzen erfolgen. Der Spielzyklus wird initiiert, nachdem der Spieler:
 - i. einen Einsatz oder eine Wette platziert und/oder
 - ii. eine „Spiel“-Schaltfläche betätigt oder eine ähnliche Handlung durchführt, um ein Spiel gemäß den Regeln des Spiels zu initiieren.
- b) Zu einem beliebigen Zeitpunkt am Beginn oder im Verlauf eines Spielzyklus getätigte oder zugesagte Einsätze müssen von der Guthabenanzeige oder vom Kontostand des Spielerguthabens abgezogen werden. Es darf kein Einsatz akzeptiert werden, der zu einem negativen Kontostand für den Spieler führt.
- c) Die folgenden Spielelemente müssen als Bestandteil eines einzelnen Spielzyklus angesehen werden:
 - i. Spiele, die einen Freispiel-Bonus/ein Freispiel-Feature auslösen sowie alle nachfolgenden Freispiele;
 - ii. „Zweitbildschirm“-Boni/Features;
 - iii. Spiele mit Spielerauswahl (z. B. Draw Poker oder Black Jack);
 - iv. Spiele, deren Regeln zusätzliche Einsätze zulassen (z. B. Blackjack, Blackjack-Versicherung oder der zweite Teil eines zweiteiligen Keno-Spiels); und
 - v. Verdopplungs-/Risiko-Features.
- d) Ein Spielzyklus muss als abgeschlossen angesehen werden, wenn alle Einsätze verloren wurden oder die endgültige Übertragung an die Guthabenanzeige oder den Kontostand des Spielers erfolgt. Der Wert jeder Prämie am Ende eines Spielzyklus wird der Guthabenanzeige oder dem Kontostand des Spielers hinzugefügt, es sei denn, es handelt sich um Merchandising oder hohe Auszahlungssummen, sofern von der Regulierungsbehörde gefordert.
- e) Es darf nicht möglich sein, innerhalb derselben Spielsitzung ein neues Spiel zu beginnen, bevor der aktuelle Spielzyklus abgeschlossen ist und die für Einsätze verfügbaren Beträge sowie der Spielverlauf aktualisiert wurden, einschließlich der oben aufgeführten Spielelemente, sofern das aktuelle Spiel durch die Handlung zum Beginnen eines neuen Spiels nicht ordnungsgemäß beendet wird. Ausnahmen sind möglich, beispielsweise wenn sich der Betreiber für einen Offline-Betrieb entscheidet, bei manuellen Abwägungen hoher Auszahlungssummen oder wenn ein Spieler weiterspielen möchte, während eine hohe Auszahlung ansteht.

4.3.4 Anzuzeigende Informationen

Eine Spielerschnittstelle muss innerhalb einer Spielsitzung die folgenden Informationen anzeigen, es sei denn, der Spieler betrachtet einen Informationsbildschirm wie ein Menü oder einen Hilfebildschirm:

- a) aktuell für Einsätze verfügbare Beträge;
- b) gespielte Stückelung (sofern zutreffend);
- c) aktueller Einsatzbetrag und Platzierung aller aktiven Einsätze oder ausreichende Anzeigeeinformationen, um diese Parameter anderweitig abzuleiten;
- d) jegliche Einsatzoptionen für den Spieler, die vor der Initiierung oder im Verlauf des Spiels bestehen;

- e) für das letzte abgeschlossene Spiel die folgenden Informationen, bis das nächste Spiel beginnt, Einsatzoptionen geändert werden oder der Spieler das Spiel verlässt;
 - i. präzise Darstellung des Spielergebnisses;
 - ii. gewonnener Betrag; und
 - iii. jegliche wirksamen Einsatzoptionen für den Spieler.

HINWEIS: Es ist akzeptabel, die Informationen über das letzte abgeschlossene Spiel zu löschen, bevor die oben genannten Bedingungen erfüllt sind, solange dieselben Informationen im Abschnitt „Spiel-Rückruf“ dieses Dokuments dem Spieler klar erkennbar zur Verfügung stehen.

4.3.5 Guthabenanzeige

Abhängig von der Implementierung innerhalb der Spielplattform können Geldbeträge aus dem Guthaben des Spielerkontos auf eine Guthabenanzeige für die Spielsitzung übertragen werden. Dies kann automatisch erfolgen, wenn der Stand des Spielerkontos automatisch an die Guthabenanzeige übertragen wird oder die Spielplattform dem Spieler Übertragungsmöglichkeiten bietet, die eine vorherige Auswahl durch den Spieler erfordern. Solche Optionen würden die Höhe des Betrags beinhalten, den der Spieler an die Guthabenanzeige der Sitzung übertragen möchte. Nach Abschluss muss der Spieler die Möglichkeit erhalten, sein Guthaben teilweise oder vollständig zurück an sein Kontoguthaben zu übertragen. Beim Verlassen einer Spielsitzung müssen alle Geldbeträge automatisch wieder dem Guthaben des Spielerkontos hinzugefügt werden. Darüber hinaus muss die Guthabenanzeige bei einer Verwendung die folgenden Anforderungen erfüllen:

- a) Die Guthabenanzeige muss für den Spieler immer dann sichtbar sein, wenn ein Einsatz getätigt werden kann, wenn eine Übertragung an das oder vom Guthaben des Spielerkontos zulässig ist oder wenn die Anzeige aktiv erhöht oder reduziert wird.
- b) Die Guthabenanzeige muss in Credits oder in einem lokalen Währungsformat angezeigt werden. Wenn die Guthabenanzeige des Spiels ein Umschalten zwischen Credits und Währung gestattet, muss diese Funktion für den Spieler leicht verständlich sein. Die Guthabenanzeige muss klar darstellen, ob die Beträge aktuell in Credits oder in der entsprechenden Währung angezeigt werden.
- c) Wenn der Betrag in lokaler Währung keinem geraden Vielfachen der Stückelung für ein Spiel entspricht oder der Credit-Betrag einen Bruchwert hat, können die Credits für das Spiel als gekürzter Wert (d. h. ohne den Bruchteil) angezeigt und für das Spiel genutzt werden. Der Bruchteil eines Credit-Betrags muss dem Spieler jedoch zur Verfügung gestellt werden, wenn das gekürzte Credit-Guthaben gleich null ist.
- d) Wenn eingeschränkte Anreizgutschriften und nicht eingeschränkte Spielergelder in einer Guthabenanzeige kombiniert werden, müssen die eingeschränkten Gutschriften gemäß den Spielregeln zuerst eingesetzt werden, bevor nicht eingeschränkte Spielergelder eingesetzt werden können.

4.4 Spielinformationen und Spielregeln

4.4.1 Spielinformationen und Spielregeln

Die folgenden Anforderungen gelten für die Spielinformationen, Illustrationen, Gewinntabellen und

Hilfe-Bildschirme, einschließlich jeglicher schriftlicher, grafischer und akustischer Informationen, die dem Spieler entweder direkt über die Spielerschnittstelle oder über eine dem Spieler zugängliche Seite angezeigt werden:

- a) Benutzeranweisungen für die Spielerschnittstelle und Spieler-Interaktionsgeräte, Gewinntabellen-Informationen und Spielregeln müssen vollständig und eindeutig sein und dürfen weder missverständlich noch unfair für den Spieler sein.
- b) Hilfebildschirm-Informationen müssen für den Spieler zugänglich sein, ohne dass Geldbeträge eingezahlt oder eingesetzt werden. Diese Informationen müssen Beschreibungen eindeutiger Spielboni/Features, Spielerweiterungen, Freispiele, Verdopplungen, automatischer Spiele, Countdown-Timer, Symbolumwandlungen, Gemeinschaftsboni, progressiver Jackpots, stufenweiser Jackpots etc. enthalten.
- c) Minimum, Maximum und andere verfügbare Einsätze müssen innerhalb der Illustrationen angegeben werden oder mit angemessenen Anweisungen für jede Einsatzoption aus diesen abgeleitet werden können.
- d) Gewinntabellen-Informationen müssen für jegliche verfügbaren Modifikatoren und/oder Einsatzoptionen alle möglichen Gewinnergebnis und -kombinationen beinhalten, ebenso wie ihre entsprechenden Auszahlungen.
- e) Die Illustrationen müssen klar vermitteln, ob Prämien in Credits, Währung oder einer anderen Einheit vorgesehen sind.
- f) Für Illustrationen, die Spielanleitungen enthalten, die explizit eine Credit-Prämie oder einen Merchandising-Preis bewerben, muss es möglich sein, die beworbene Prämie/den beworbenen Preis in einem einzelnen Spiel oder eine Reihe von Spielen zu gewinnen, die durch ein initiiertes Spiel aktiviert wurde, wenn Boni/Features oder andere Spieloptionen enthalten sind, oder die Illustrationen müssen die Kriterien für den Gewinn der beworbenen Prämie/des beworbenen Preises klar darlegen.
- g) Das Spiel muss alle Änderungen des Prämienwerts widerspiegeln, die im Verlauf des Spiels erfolgen können. Dies kann mithilfe einer digitalen Anzeige an einer gut sichtbaren Stelle oder in der Spielerschnittstelle erfolgen. Das Spiel muss die Kriterien für jegliche Änderungen des Prämienwerts klar zum Ausdruck bringen.
- h) Akustische Spielanleitungen müssen zusätzlich in schriftlicher Form in den Illustrationen angezeigt werden.
- i) Die Spielanleitungen müssen in einer Farbe dargestellt werden, die sich von der Hintergrundfarbe abhebt, um zu gewährleisten, dass alle Informationen deutlich sichtbar/lesbar sind.
- j) Die Illustrationen müssen die Regeln für die Auszahlung von Prämien deutlich darstellen. Wenn eine bestimmte Gewinnkombination ausgezahlt wird, wo mehrere Gewinne möglich sind, muss die Zahlungsmethode beschrieben werden.
 - i. Die Illustrationen müssen den Umgang mit sich überschneidenden Spielergebnissen klar kommunizieren. Beispielsweise ob ein Straight Flush sowohl als Flush als auch als Straight angesehen wird, oder ob für 3/4/5 Gleiche eine Auszahlung für alle Gleichen oder lediglich für den höchsten Wert erfolgt. Wenn eine Gewinnlinie mehr als eine solche Gewinnkombination aufweisen kann, muss angegeben werden, wenn nur die höchste Gewinnkombination pro Linie ausgezahlt wird.
 - ii. Wenn das gleiche Symbol gleichzeitig Bestandteil eines Liniengewinns und eines Scatter-Gewinns sein kann oder Linien- und Scatter-Gewinne gleichzeitig auf derselben Linie

- auftreten, muss die Illustration darüber informieren, ob der Spieler beide Gewinne erhält oder lediglich den höheren der beiden Gewinne.
- iii. Die Illustrationen müssen den Umgang mit sich überschneidenden Scatter-Gewinnen klar kommunizieren. Beispielsweise müssen die Illustrationen Informationen enthalten, ob bei Kombinationen von Scatter-Symbolen alle möglichen Prämien ausgezahlt werden oder lediglich die höchste Prämie.
 - k) Wenn die Illustrationen Multiplikator-Anweisungen enthalten, muss klar sein, worauf der Multiplikator angewendet wird und worauf nicht.
 - l) Alle Spielsymbole/Objekte müssen dem Spieler deutlich angezeigt werden und dürfen nicht missverständlich sein.
 - i. Spielanleitungen, die speziell für ein oder mehrere Symbole/Prämien vorgesehen sind, müssen diesen Symbolen/Prämien klar zugeordnet werden. Dies kann beispielsweise durch entsprechende Rahmen und Felder erfolgen. Darüber hinaus können zusätzliche Formulierungen wie „diese Symbole“ verwendet werden.
 - ii. Wenn sich Spielanleitungen auf ein bestimmtes Symbol beziehen und der ausgeschriebene Name für das Symbol mit einem anderen Symbol verwechselt werden oder andere Eigenschaften implizieren kann, muss die visuelle Darstellung der Anleitung klar angeben, auf welches Symbol sich die Anleitung bezieht.
 - iii. Spielsymbole und Objekte müssen in allen Illustrationen ihre Form behalten, mit Ausnahme laufender Animationen. Kein Symbol, das während eines Animationsprozesses seine Form oder Farbe ändert, darf auf eine Weise erscheinen, die fehlinterpretiert werden kann und eine Verwechslung mit anderen Symbolen in der Gewinnntabelle ermöglicht.
 - iv. Wenn sich die Funktion eines Symbols ändert (z. B. ein nicht ersetzendes Symbol wird während eines Features zu einem ersetzenden Symbol) oder sich das Erscheinungsbild des Symbols verändert, müssen die Illustrationen diese Änderung der Funktion oder des Erscheinungsbildes sowie jegliche hiermit verbundenen besonderen Bedingungen klar widerspiegeln.
 - v. Falls hinsichtlich der Position und/oder des Erscheinungsbildes eines beliebigen Symbols Einschränkungen bestehen, müssen diese Einschränkungen in den Illustrationen angegeben werden. Wenn beispielsweise ein Symbol nur in einem Bonusspiel oder auf einer bestimmten Walze verfügbar ist, muss die Illustration darauf hinweisen.
 - m) Die Illustration muss klare Angaben enthalten, welche Symbole/Objekte als Ersatz oder Wild fungieren können und in welchen Gewinnkombinationen der Ersatz oder das Wild-Symbol angewendet werden kann; diese Beschreibung muss alle Phasen des Spiels behandeln, in denen Wild- oder Ersatzsymbole erscheinen können.
 - n) Die Illustration muss klare Angaben enthalten, welche Symbole/Objekte als Scatter fungieren können und in welchen Gewinnkombinationen das Scatter-Symbol angewendet werden kann.
 - o) Die Illustration muss klare Informationen in schriftlicher und/oder grafischer Form enthalten, um die Reihenfolge, in der Symbole erscheinen müssen, um eine Prämie zu vergeben oder ein Feature auszulösen, klar zu erläutern, einschließlich Zahlen zur Anzeige, wie vielen korrekten Symbolen/Objekten jedes Muster entspricht.
 - p) Das Spiel darf keine Werbung für „zukünftige Gewinne“ enthalten, wie beispielsweise „dreifache Auszahlung in Kürze“, sofern die Werbung nicht präzise und mathematisch demonstrierbar ist oder der Spieler keine direkte Werbung des aktuellen Fortschritts für diesen Gewinn erhält (z. B. bei zwei von vier gesammelten Tokens, die für den Gewinn einer Prämie erforderlich sind).
 - q) Die Spielillustration muss dem Spieler alle nicht einsatzbezogenen Kaufoptionen und deren Wert

in Credits oder lokaler Währung klar erläutern.

- r) Die Illustration muss jegliche restriktiven Features des Spielverlaufs wie z. B. Begrenzungen der Spieldauer, maximale Gewinnwerte etc. erklären, die als Element des Spielaufbaus implementiert sind.
- s) Es müssen ausreichende Informationen in Bezug auf jegliche Anpassungen von Prämienauszahlungen vorhanden sein, wie durch den Betreiber erhobene Rakes, Provisionen oder Gebühren, sofern zutreffend.

4.4.2 Spiele mit mehreren Einsätzen

Die folgenden Anforderungen müssen, sofern für den jeweiligen Spielaufbau relevant, für Spiele gelten, in denen mehrere unabhängige Einsätze gleichzeitig für beworbene Prämien gelten:

- a) Jeder einzelne getätigte Einsatz muss klar angegeben werden, so dass für den Spieler zweifelsfrei erkennbar ist, welche Einsätze in welcher Höhe getätigt wurden;
- b) der Gewinnbetrag für jeden separaten Einsatz und der Gesamtgewinnbetrag müssen auf demselben Bildschirm angezeigt werden; und
- c) jeder Prämiegewinn muss dem Spieler auf eine Weise angezeigt werden, welche die Prämie klar dem entsprechenden Einsatz zuordnet. Wenn Gewinne mehreren Einsätzen zugeordnet sind, kann im Gegenzug jeder Einsatz angezeigt werden. In Fällen, in denen umfangreiche Informationen vermittelt werden müssen, kann ein zusammenfassender Bildschirm ausreichend sein. Alle Ausnahmen werden auf fallweiser Basis durch das unabhängige Prüflabor beurteilt.

4.4.3 Linienspiele

Die folgenden Anforderungen müssen, sofern für den jeweiligen Spielaufbau relevant, für Linienspiele gelten:

- a) Bei Mehrfach-Linien-Spielen muss eine Zusammenfassung der verfügbaren Gewinnlinien angezeigt werden, aus denen Gewinnkombinationen gebildet werden können;
- b) jede einzelne zu spielende Linie muss im Spiel klar angegeben werden, so dass für den Spieler zweifelsfrei erkennbar ist, auf welche Linien gesetzt wird. Das Anzeigen der Anzahl von Linien, auf die gesetzt wurde, ist ausreichend, um diese Anforderung zu erfüllen;
- c) bei Spielen, die den Einsatz mehrerer Credits auf ausgewählten Linien gestatten, muss die Illustration:
 - i. Bei linearen Gewinnen klar verdeutlichen, dass der Gewinn/die Gewinne für jede ausgewählte Linie mit dem Einsatzmultiplikator multipliziert wird/werden; oder
 - ii. bei nicht linearen Gewinnen über alle möglichen Einsätze und ihre Prämien informieren;
- d) der Einsatzmultiplikator muss angezeigt werden. Es ist akzeptabel, wenn dieser einfach aus anderen angezeigten Informationen abgeleitet werden kann;
- e) die Illustration muss jegliche Regeln und/oder Einschränkungen in Bezug darauf enthalten, wie Gewinne gewertet werden, einschließlich folgender Informationen:
 - i. wie Liniengewinne gewertet werden (d. h. von links nach rechts, von rechts nach links oder in beiden Richtungen);
 - ii. wie einzelne Symbole gewertet werden (d. h. ob Gewinne nur auf benachbarten Walzen oder als Scatter-Gewinne gewertet werden); und

- f) Gewinnlinien müssen für den Spieler klar erkennbar sein. Bei Gewinnen auf mehreren Linien muss im Gegenzug jede Gewinnlinie angezeigt werden. Diese Anforderung schließt weder andere intuitive Methoden der Anzeige von Liniengewinnen aus, wie z. B. die Gruppierung häufiger Gewinntypen, noch verbietet sie die Möglichkeit für den Spieler, eine detaillierte Ergebnisanzeige von Liniengewinnen zu umgehen, sofern unterstützt.

4.4.4 Kartenspiele

Die folgenden Anforderungen müssen, sofern für den jeweiligen Spielaufbau relevant, für Spiele gelten, die das Ziehen von Karten aus einem oder mehreren Kartenstapeln beinhalten:

- a) Zu Beginn jedes Spiels und/oder jeder Hand müssen die Karten aus (einem) zufällig gemischtem Stapel(n) gezogen werden. Es ist akzeptabel, Zufallszahlen für Ersatzkarten zu ziehen, wenn die Zufallszahlen für die erste Hand gezogen werden, sofern die Ersatzkarten bei Bedarf sequenziell genutzt werden und die gespeicherten RNG-Werte verschlüsselt sind;
- b) aus dem/den Stapel(n) entfernte Karten dürfen nicht zurück in den/die Stapel gelangen, es sei denn, dies ist durch die Spielregeln vorgesehen;
- c) der/die Stapel dürfen nicht erneut gemischt werden, es sei denn, dies ist durch die Spielregeln vorgesehen;
- d) das Spiel muss den Spieler über die Anzahl von Karten in einem Stapel und die Anzahl von Stapeln im Spiel informieren;
- e) Kartenwert und -farbe müssen auf der Vorderseite der Karte klar erkennbar sein; und
- f) Joker und Platzhalter müssen von allen anderen Karten unterscheidbar sein.

4.4.5 Pokerspiele

Die folgenden Anforderungen gelten, sofern für den jeweiligen Spielaufbau relevant, für Simulationen von Pokerspielen:

- a) Die Illustration muss klare Angaben enthalten, welche Pokervariante gespielt wird und welche Regeln gelten;
- b) Regeln für Platzhalter müssen auf den Hilfebildschirmen klar erläutert werden; und
- c) gehaltene und nicht gehaltene Karten, einschließlich empfohlener gehaltener Karten, sofern zulässig, müssen auf dem Bildschirm klar gekennzeichnet sein. Die Methode zum Ändern des Status einer ausgewählten Karte muss dem Spieler klar verdeutlicht werden.

4.4.6 Blackjack-Spiele

Die folgenden Anforderungen gelten, sofern für den jeweiligen Spielaufbau relevant, für Simulationen von Blackjack-Spielen:

- a) Regeln für eine Versicherung müssen deutlich erklärt werden, sofern sie verfügbar ist;
- b) die Regeln zum Teilen von Paaren muss erklärt werden und Folgendes beinhalten:
 - i. Bei geteilten Assen wird jedem Ass nur eine Karte zugeteilt, wenn dies die Spielregel ist;
 - ii. weiteres Teilen, wenn verfügbar;
 - iii. Einsatzverdopplung nach dem Teilen, wenn verfügbar;

- c) die Regeln zur Einsatzverdopplung müssen klar erläutert werden, einschließlich Einschränkungen bei welchen Gesamtwerten eine Einsatzverdopplung ausgewählt werden kann;
- d) jegliche Einschränkung der Anzahl von Karten, die vom Spieler und/oder Geber gezogen werden kann, muss erklärt werden, einschließlich Verkündung der Gewinner (sofern vorhanden), wenn das Limit erreicht wurde (z. B. fünf Karten unter 21);
- e) Regeln für Aufgabe, sofern vorhanden, müssen erklärt werden;
- f) wenn Paare geteilt wurden, müssen die Ergebnisse für jede Hand angezeigt werden (z. B. Gesamtpunkte, resultierende Gewinn- oder Verlustkategorie, eingesetzter Betrag);
- g) Sonderregeln, sofern vorhanden, müssen klar erläutert werden; und
- h) sämtliche zu einem beliebigen Zeitpunkt verfügbaren Spieleroptionen müssen in der Illustration dargestellt werden.

4.4.7 Roulette-Spiele

Die folgenden Anforderungen gelten, sofern für den jeweiligen Spielaufbau relevant, für Simulationen von Roulette-Spielen:

- a) Die Methode zur Auswahl einzelner Einsätze muss in den Spielregeln erklärt werden;
- b) bereits vom Spieler ausgewählte Einsätze müssen auf dem Bildschirm angezeigt werden; und
- c) das Ergebnis jedes Drehs des Roulettekessels muss dem Spieler klar angezeigt werden.

4.4.8 Würfelspiele

Die folgenden Anforderungen gelten, sofern für den jeweiligen Spielaufbau relevant, für Simulationen von Würfelspielen:

- a) Jede Würfelseite muss eine klare Darstellung der Anzahl der Punkte oder anderer Symbole für ihren Wert aufweisen;
- b) es muss klar erkennbar sein, welche Seite des Würfels nach dem Würfeln nach oben weist; und
- c) das Ergebnis jedes Wurfs muss klar sichtbar sein oder angezeigt werden.

4.4.9 Sport-/Rennspiele

Die folgenden Anforderungen gelten, sofern für den jeweiligen Spielaufbau relevant, für Simulationen von Sport- oder Rennspielen:

- a) Jeder Teilnehmer an einem Spiel muss ein einzigartiges Erscheinungsbild aufweisen, sofern auf den Einsatz anwendbar;
- b) die Ergebnisse eines Spiels müssen klar sein und dürfen keinen Raum für Fehlinterpretationen durch den Spieler bieten;
- c) wenn Prämien für Kombinationen ausgezahlt werden müssen, an denen andere Teilnehmer als nur der Erstplatzierte beteiligt sind, muss die Reihenfolge der möglicherweise an diesen Prämien beteiligten Teilnehmer auf dem Bildschirm klar angezeigt werden (z. B. Ergebnis 8-4-7); und
- d) die Regeln für jegliche exotischen Wettoptionen (z. B. Perfecta, Trifecta, Quinella etc.) sowie die erwarteten Auszahlungen müssen in den Illustrationen klar erläutert werden.

4.4.10 Spiele mit Kugel-/Zahlenziehungen

Die folgenden Anforderungen müssen, sofern für den jeweiligen Spielaufbau relevant, für Spiele gelten, die das Ziehen von Kugeln oder Zahlen aus einem Pool beinhalten:

- a) Simulierte Kugeln/Zahlen müssen aus einem zufällig gemischten Pool gezogen werden, der aus dem vollständigen Satz von Kugeln/Zahlen besteht, die auf die Spielregeln anwendbar sind;
- b) zu Beginn jedes Spiels werden nur die Kugeln/Zahlen dargestellt, die auf das Spiel anwendbar sind. bei Spielen mit Boni/Features und zusätzlichen Kugeln/Zahlen, die ausgewählt werden, müssen sie der ursprünglichen Auswahl entnommen werden, sofern nicht durch die Spielregeln anders zulässig;
- c) der Pool darf nicht erneut gemischt werden, es sei denn, dies ist durch die Spielregeln vorgesehen; und
- d) alle Kugeln/Zahlen müssen dem Spieler deutlich angezeigt werden.

4.4.11 Keno/Bingo/Lotteriespiele

Die folgenden Anforderungen gelten, sofern für den jeweiligen Spielaufbau relevant, für Simulationen von Keno, Bingo oder Lotteriespielen, bei denen Kugeln oder Zahlen gezogen werden und ein Spieler versucht, die ausgewählten Kugeln/Zahlen vorherzusagen:

- a) Jede Auswahl des Spielers muss auf dem Spielbildschirm klar erkennbar sein. Wenn das Spiel mehrere Spielerkarten nutzt, ist es akzeptabel, dass die jeweiligen Auswahlen des Spielers durch Umdrehen oder Verschieben der Karten zugänglich sind;
- b) die gezogenen Zahlen müssen auf dem Bildschirm klar erkennbar sein;
- c) das Spiel muss gezogene Zahlen, die der Spielervorhersage entsprechen, hervorheben;
- d) besondere Treffer, sofern vorhanden, müssen klar erkennbar sein;
- e) der Bildschirm muss klare Angaben enthalten, wie viele Punkte ausgewählt und wie viele Treffer erzielt wurden; und
- f) die Regeln für den Kauf zusätzlicher Spiel-Features (sofern vorhanden) müssen erklärt werden.

4.4.12 Rubbellos-Spiele

Die folgenden Anforderungen gelten, sofern für den jeweiligen Spielaufbau relevant, für Simulationen von Rubbellos-Spielen, in denen der Spieler ein elektronisches Rubbellos erwirbt:

- a) Elektronische Rubbellos-Spiele müssen statt auf Spielerfähigkeiten auf Zufall basieren;
- b) eine präzise Definition, welche Auswahl der Spieler treffen muss, um das Spiel abzuschließen, muss in der Illustration enthalten sein;
- c) bei Spielen, die beliebte Praxisthemen nutzen (Karten, Würfel etc.), jedoch keinen tatsächlichen Spielverlauf und tatsächlichen Wahrscheinlichkeiten widerspiegeln, muss der Illustration ein Disclaimer hinzugefügt werden, der aussagt, dass die Ergebnisse nicht die Wahrscheinlichkeiten aufweisen, die üblicherweise von diesem Spiel zu erwarten wären; und
- d) nachdem der Spieler ein elektronisches Rubbellos erworben hat, müssen ihm das Ergebnis und der Preis des Spiels offengelegt werden. Der Spieler kann mit dem elektronischen Rubbellos

interagieren müssen oder nicht, um die Gewinn-/Verlustergebnisse offenzulegen, wie von der Regulierungsbehörde gefordert.

4.4.13 Multiplayer-Spiele

Die folgenden Anforderungen müssen, sofern für den jeweiligen Spielaufbau relevant, für Multiplayer-Spiele gelten:

- a) Das Multiplayer-Spiel muss so aufgebaut sein, dass die Handlungen oder Ergebnisse eines anderen Spielers nicht das Ergebnis/die Ergebnisse jeglicher anderer Spieler beeinträchtigt, sofern nicht durch die Spielregeln anderweitig festgelegt; und
- b) jedes Multiplayer-Spiel muss für jeden Spieler eine Möglichkeit bieten, zu erfahren, wann das nächste Spiel beginnt.

HINWEIS: Bitte beachten Sie den Abschnitt „Peer-to-Peer (P2P) Spielsitzungen“ dieses Kapitels, um mehr über spezielle und ergänzende Anforderungen an Multiplayer-Spiele zu erfahren, bei denen Spieler gegeneinander antreten.

4.5 Spielergesult durch Zufallszahlengenerator (RNG)

4.5.1 RNG und Auswertung des Spielergesultes

Die Auswertung des Spielergesultes mithilfe eines RNG muss den folgenden Regeln entsprechen:

- a) Wenn mehr als ein RNG zur Bestimmung der verschiedenen Spielergesultes genutzt wird, muss jeder RNG separat ausgewertet werden; und
- b) wenn jede Instanz eines RNG identisch ist, aber eine andere Implementierung innerhalb des Spiels beinhaltet, muss jede Implementierung separat ausgewertet werden.

4.5.2 Spielauswahl

Die Bestimmung von Ereignissen, die zu einem monetären Gewinn führen, darf nicht durch andere Faktoren beeinflusst, beeinträchtigt oder gesteuert werden als die in Übereinstimmung mit den folgenden Anforderungen durch einen zulässigen RNG ausgewählten Werten:

- a) Bei Abrufen des RNG darf das Spiel nicht die zur Auswahl stehenden Ergebnisse einschränken, sofern dies nicht durch den Spielaufbau vorgesehen ist;
- b) das Spiel darf keine vom RNG ausgewählten Ergebnisse aufgrund adaptiven Verhaltens modifizieren oder verwerfen. Darüber hinaus müssen die Ergebnisse wie durch die Spielregeln vorgegeben genutzt werden;
- c) nach Auswahl des Spielergesultes darf das Spiel keine „Beinahetreffer“ anzeigen, wenn dies zu einer variablen Sekundärentscheidung führt, welche die dem Spieler angezeigten Ergebnisse beeinflusst. Wenn beispielsweise der RNG ein Verlusteresult auswählt, darf das Spiel kein anderes Verlusteresult ersetzen, um dem Spieler ein anderes als das ursprünglich ausgewählte anzuzeigen;

- d) außer wenn durch die Spielregeln vorgesehen, müssen Zufallsereignisse unabhängig sein und dürfen nicht mit jeglichen anderen Ereignissen innerhalb desselben Spiels oder mit Ereignissen in vorherigen Spielen zusammenhängen:
 - i. Ein Spiel darf nicht basierend auf der Historie in vorherigen Spielen erhaltener Prämien die Wahrscheinlichkeit für einen Bonus/ein Feature verändern;
 - ii. ein Spiel darf nicht basierend auf vorangegangenen Auszahlungen seine theoretische Ausschüttungsquote ändern;
- e) keine zugeordneten Geräte, die in Verbindung mit einer Spielplattform genutzt werden, dürfen das Verhalten des Spiel-RNGs und/oder den Prozess der Zufallsauswahl beeinflussen oder verändern, sofern dies nicht autorisiert oder konzeptionell vorgesehen ist; und
- f) Zufallsereignisse dürfen nicht von der effektiven Bandbreite, Linknutzung, Bit-Fehlerrate oder anderen Eigenschaften des Kommunikationskanals zwischen der Spielplattform und dem Remote-Spieler-Gerät beeinflusst werden. Der Spieler muss informiert werden, wenn diese Eigenschaften jegliche anderen Auswirkungen auf das Spiel haben oder zu haben scheinen, wie beispielsweise bei der Entscheidungsfindung, bei der Geschwindigkeit ein bedeutender Faktor ist, bei der Aktualisierung der Jackpot-Anzeigen oder Spielunterbrechung bei Multiplayer-Spielen.

4.6 Spiel-Fairness

4.6.1 Spiel-Fairness

Die folgenden Anforderungen müssen für die Spiel-Fairness gelten:

- a) Spiele, die so konzipiert sind, dass sie einem Spieler den Eindruck vermitteln, das Spielergebnis durch Fähigkeiten oder Geschicklichkeit kontrollieren zu können, obwohl dies tatsächlich nicht der Fall ist (d. h. das Spielergebnis ist zufällig und der Eindruck von Fähigkeitselementen dient lediglich Unterhaltungszwecken), müssen diese Tatsache innerhalb der Hilfebildschirme des Spiels vollständig offenlegen. Dies gilt nicht für Spiele, die keine Basis für Fähigkeitselemente bieten und/oder die keiner Strategie folgen. Ein Beispiel wäre ein einfaches Spiel mit Bonusauswahl, bei dem für den Spieler offensichtlich ist, dass das Ergebnis auf Glück basiert;
- b) die Spiele dürfen keinerlei verborgenen Quellcode enthalten, der von einem Spieler dazu genutzt werden kann, die Spielregeln und/oder das durch den Spielaufbau vorgesehene Verhalten zu umgehen. Diese Anforderung schließt keine hinreichend identifizierbaren „Suchfunktionen“ eines Spiels aus, die vom Spielaufbau her vorgesehen sind, jedoch möglicherweise nicht dokumentiert oder dem Spieler nicht bekannt sind; und
- c) Das Endergebnis jedes Spiels muss ausreichend lange angezeigt werden, so dass ein Spieler eine angemessene Möglichkeit erhält, das Ergebnis des Spiels zu verifizieren. Diese Anforderung schließt keine Option für den Spieler aus, die Ergebnisanzeige zu umgehen.

4.6.2 Simulation physischer Objekte

Wenn ein Spiel eine grafische Darstellung oder Simulation eines physischen Objekts beinhaltet, um das Spielergebnis zu bestimmen, müssen die durch die Simulation dargestellten Verhaltensweisen denen des realen Objekts entsprechen, sofern in der Spielillustration nicht anders angegeben. Diese

Anforderung gilt nicht für grafische Darstellungen oder Simulationen, die lediglich Unterhaltungszwecken dienen. Die folgenden Anforderungen müssen für die Simulation gelten:

- a) Die Wahrscheinlichkeit, dass ein beliebiges Ereignis in der Simulation eintritt, das sich auf das Spielergebnis auswirkt, muss den Eigenschaften des physischen Objekts entsprechen, sofern dem Spieler nicht anderslautend mitgeteilt;
- b) wenn das Spiel mehrere physische Objekte simuliert, von denen normalerweise erwartet würde, dass sie basierend auf den Spielregeln voneinander unabhängig sind, muss jede Simulation unabhängig von allen anderen Simulationen sein; und
- c) wenn das Spiel physische Objekte simuliert, die keine vorherigen Ereignisse speichern, muss das Verhalten der simulierten Objekte unabhängig von ihrem vorherigen Verhalten sein, so dass das Verhalten nicht adaptiv und nicht vorhersehbar ist, sofern dem Spieler nicht anderslautend mitgeteilt.

4.6.3 Physik-Engine

Spiele können eine „Physik-Engine“ nutzen, bei der es sich um spezielle Software handelt, die eine physische Umgebung nachstellt oder simuliert, einschließlich Verhaltensweisen wie Bewegung, Gravitation, Geschwindigkeit, Beschleunigung, Trägheit, Flugbahnen etc. Eine Physik-Engine muss so konzipiert sein, dass sie ein konsistentes Spielverhalten und eine konsistente Spielumgebung bereitstellt, sofern der Spieler durch die Spiel-Illustration nicht anderslautend informiert wurde. Eine Physik-Engine kann die Zufallseigenschaften eines RNG nutzen, um Auswirkungen auf das Spielergebnis zu erzielen, wobei die „Anforderungen an Zufallsgeneratoren“ Anwendung finden.

HINWEIS: Implementierungen einer Physik-Engine in einem Spiel werden auf fallweiser Basis durch das unabhängige Prüflabor beurteilt.

4.6.4 Live-Spiel-Korrelation

Sofern in der Spiel-Illustration nicht anders angegeben, müssen, wenn die Spielplattform ein Spiel anbietet, das als Simulation eines Live-Casinos erkennbar ist, wie beispielsweise Poker, Black Jack, Roulette etc., dieselben Wahrscheinlichkeiten wie im Live-Spiel auch für das simulierte Spiel gelten. Beispielsweise muss beim Roulette bei Vorhandensein einer einzelnen Null (Zero – 0) und einer doppelten Null (Doppel-Zero – 00) auf dem Kessel die Wahrscheinlichkeit für eine bestimmte Zahl bei 1 zu 38 liegen. Die Wahrscheinlichkeit für das Ziehen einer oder mehrerer bestimmter Karten beim Poker muss die gleiche sein wie im Live-Spiel.

4.6.5 Wahrscheinlichkeit von Zufallsereignissen

Bei Spielen, die ein Zufallsereignis oder ein Glückselement beinhalten, das sich auf das Ergebnis auswirkt, muss die mathematische Wahrscheinlichkeit jedes eintretenden Zufallsereignisses für ein gebührenpflichtiges Spiel konstant sein, sofern in der Spiel-Illustration nicht anders angegeben.

4.7 Spieldauszahlungs-Raten, Wahrscheinlichkeiten und Nicht-Cash-Prämien

4.7.1 Software-Anforderungen für prozentuale Auszahlungen

Jedes Hausbank-Spiel muss während der erwarteten Lebensdauer des Spiels theoretisch eine Auszahlungsquote von mindestens fünfundsiebzig Prozent (75 %) aufweisen, sofern nicht durch die Regulierungsbehörde anders vorgegeben. Progressive Jackpots, stufenweise Jackpots, Anreizprämien, Merchandising-Artikel etc. dürfen nicht in die prozentuale Auszahlung eingeschlossen werden, wenn sie außerhalb des Spiels vergeben werden, es sei denn, dies ist für den Betrieb erforderlich.

- a) Die prozentuale Mindestanforderung muss für alle Einsatzkonfigurationen erfüllt werden. Wenn ein Spiel mit beliebigem Einsatzniveau, beliebiger Linienkonfiguration etc. während seiner Lebensdauer kontinuierlich gespielt wird, müssen die Prozentanforderungen erfüllt werden.
- b) Spiele, die durch Spielerfähigkeiten beeinflusst werden, müssen die prozentuale Mindestanforderung erfüllen, wenn sie eine optimale Spielmethode nutzen, die die größtmögliche Ausschüttungsquote innerhalb eines Zeitraums kontinuierlichen Spielens bietet.
- c) Wenn progressive Jackpots und stufenweise Jackpots in die Berechnung der Ausschüttungsquote (RTP) für das Spiel einbezogen werden, muss die prozentuale Mindestanforderung unter Nutzung der geringsten verfügbaren Jackpot-Parameter während der erwarteten Lebensdauer des Spiels erfüllt werden.
- d) Wenn von der Regulierungsbehörde gestattet, muss die Mindest-RTP für Spiele, in denen die obigen prozentualen Mindestanforderungen nicht erfüllt werden (z. B. elektronische Rubbellos- oder Lotteriespiele), dem Spieler angezeigt werden und die Anforderungen für die „Anzeige der Ausschüttungsquote (RTP)“ muss erfüllt werden.

HINWEIS: Nach Ermessen der Regulierungsbehörde kann das unabhängige Prüflabor einen alternativen Ansatz für die Berechnung der prozentualen Ausschüttung anwenden.

4.7.2 Anzeige der Ausschüttungsquote (RTP)

Eine Regulierungsbehörde kann nach eigenem Ermessen vorschreiben, dass die Illustrationen die RTP für jedes Hausbank-Spiel enthält. Wenn die RTP angezeigt wird, müssen folgende Anforderungen erfüllt werden:

- a) Die Illustration muss vollständig erklären, wie die angezeigte RTP ermittelt wurde (d. h. Minimum, Maximum, Durchschnitt etc.) und somit erklären, wie der Spieler diese erzielen kann (d. h. Einsatzanforderungen).
- b) Bei Spielen, die durch Spielerfähigkeiten beeinflusst werden, muss die angezeigte RTP auf einer speziell in den Spielregeln dargelegten Strategie oder einer optimalen Strategie basieren, die sich aus den Spielregeln ableiten lässt.
- c) Bei Spielen, die progressive Jackpots oder stufenweise Jackpots, zeitlich begrenzte Prämien oder andere Boni/Features anbieten, muss der variable Anteil solcher Prämien an der angezeigten RTP klar offengelegt werden.
- d) Bei Spielen, die Bonus-/Feature-Spiele anbieten, die den Einsatz zusätzlicher Credits erfolgen, muss bei der angezeigten RTP berücksichtigt werden, dass ein zusätzlicher Einsatz getätigt wurde, sofern nicht anders angegeben.

- e) Wenn die angezeigte RTP die tatsächliche RTP darstellt, muss die Anzahl der Spiele in Verbindung mit dieser Berechnung gemeinsam mit dem Zeitraum angegeben werden, in dem die Spiele gespielt wurden.

4.7.3 Wahrscheinlichkeiten

Die Wahrscheinlichkeiten, die höchste angegebene, allein auf Glück basierende Prämie zu erhalten, müssen mindestens in einhundert Millionen (100.000.000) Spielen auftreten, sofern die Spiel-Illustration die tatsächlichen Wahrscheinlichkeiten nicht für den Spieler klar erkennbar ausweist. Dies gilt nicht für mehrere Prämien, die gemeinsam im selben Spiel gewonnen wurden, wobei der aggregierte Preis nicht angegeben ist. Diese Wahrscheinlichkeitsregel darf nicht auf Spiele angewendet werden, die es einem Spieler ermöglichen, die höchste angegebene Prämie mithilfe eines Bonus/Features mehrmals zu gewinnen. Diese Regel gilt für alle Einsatzkategorien, in denen die höchste angegebene Prämie gewonnen werden kann. Wenn die höchste angegebene Prämie innerhalb eines Bonus/Features gewonnen werden kann, muss die Berechnung der Wahrscheinlichkeiten die Wahrscheinlichkeiten für den Bonus/das Feature beinhalten, einschließlich der Wahrscheinlichkeiten für das Gewinnen der Prämie. Diese Regel gilt nicht für Anreizprämien.

4.7.4 Einschränkungen für Prämien

Einschränkungen der Prämienbeträge anstelle von Merchandise-, Jahresbeitrags- oder Zahlungsplänen müssen dem Spieler innerhalb des Spielthemas, das einen solchen Preis anbietet, deutlich erklärt werden.

4.8 Bonus-/Feature-Anforderungen

4.8.1 Bonus-/Feature-Spiele

Spiele, die einen Bonus/ein Feature anbieten, müssen die folgenden Anforderungen erfüllen:

- a) Ein Spiel, das einen anderen Bonus/ein anderes Feature anbietet als die zufällig auftretenden, muss dem Spieler ausreichende Informationen zum aktuellen Status für das Auslösen des nächsten Bonus/Features anzeigen;
- b) wenn ein Spiel das Erreichen mehrerer Ziele für die Aktivierung eines Bonus/Features oder das Ausgeben einer Prämie erfordert, muss die Anzahl der zu erreichenden Ziele, um den Bonus/das Feature auszulösen oder die Prämie zu gewinnen, an jedem Punkt gemeinsam mit der bereits gesammelten Anzahl angezeigt werden;
- c) das Spiel muss dem Spieler klar verdeutlichen, dass er sich in einem Bonus-/Feature-Modus befindet;
- d) wenn ein Spiel einen Bonus/ein Feature anbietet, der/das dem Spieler ermöglicht, eine oder mehrere Walzen/Karten/Symbole für einen Neudreh oder ein erneutes Ziehen zu halten, müssen die gehaltenen Walzen/Karten/Symbole klar angegeben und die Methode zum Ändern der gehaltenen Elemente muss dem Spieler deutlich erklärt werden;
- e) wenn ein Bonus/Feature nach Ansammeln einer bestimmten Anzahl von Ereignissen/Symbolen oder Kombinationen aus Ereignissen/Symbolen unterschiedlicher Art in mehreren Spielen

- ausgelöst wird, darf die Wahrscheinlichkeit für ähnliche Ereignisse/Symbole mit fortschreitendem Bonus nicht sinken, sofern dem Spieler nicht anders mitgeteilt; und
- f) wenn ein Bonus/Feature aus mehreren Ereignissen oder Drehs besteht, muss ein Zähler verwendet und dem Spieler angezeigt werden, um auf die Anzahl der anfänglich vergebenen Drehs sowie die Anzahl der verbleibenden Drehs im Bonus-/Feature-Spiel oder alternativ auf die Anzahl bereits gespielter Drehs hinzuweisen.

4.8.2 Spielerauswahl oder Interaktion in einem Bonus/Feature

Spiele, die einen Bonus/ein Feature anbieten, der/das eine Spielerauswahl oder eine Interaktion erfordert, dürfen nicht über eine automatische Auswahl oder Initiierung des Bonus/Features verfügen, sofern das Spiel nicht eine der nachstehend aufgeführten Anforderungen erfüllt und den Mechanismus für die automatische Initiierung oder Auswahl in der Illustration erklärt:

- a) Dem Spieler wird eine Auswahl angezeigt und er bestätigt über das Betätigen einer Schaltfläche oder eine andere Spieler-Interaktion ausdrücklich seine Absicht, dass das Spiel den Bonus/das Feature automatisch initiiert;
- b) der Bonus/das Feature bietet dem Spieler nur eine Auswahl, d. h. Betätigen der Schaltfläche zum Drehen des Rades. In diesem Fall kann im Rahmen des Bonus/Features nach Ablauf einer Zeitspanne von mindestens zwei Minuten eine automatische Initiierung erfolgen; oder
- c) der Bonus/das Feature wird als Teil eines Gemeinschaftsbonus angeboten, der zwei oder mehr Spieler umfasst und wo sich die Verzögerung einer angebotenen Auswahl oder Spiel-Initiierung direkt auf die Möglichkeit anderer Spieler auswirkt, ihren Bonus/ihr Feature fortzusetzen. Vor der automatischen Auswahl oder Initiierung eines Gemeinschaftsbonus muss der Spieler auf die verbleibende Zeitspanne aufmerksam gemacht werden, innerhalb derer er seine Auswahl treffen oder das Spiel initiieren muss.

4.8.3 Zusätzlich während eines Bonus/Features eingesetzte Credits

Wenn ein laufender Bonus/laufendes Feature den Einsatz zusätzlicher Geldbeträge erfordert, um fortgesetzt zu werden, muss der Spieler die Möglichkeit erhalten, nicht teilzunehmen. Wenn alle Gewinne aus dem laufenden Spiel zu einer temporären „Gewinn“-Anzeige zusammengefasst werden, statt direkt der Guthabenanzeige oder dem Kontoguthaben des Spielers hinzugefügt zu werden, muss das Spiel:

- a) eine Möglichkeit bieten, die Gewinne auf der temporären „Gewinn“-Anzeige einzusetzen (d. h. Geldbeträge der Guthabenanzeige oder dem Guthaben des Spielerkontos hinzufügen), zum Beispiel in Situationen, in denen der Spieler über kein ausreichendes Guthaben verfügt, um den Bonus/das Feature abzuschließen, oder um dem Spieler die Möglichkeit zu bieten, Geldbeträge der Guthabenanzeige oder dem Guthaben des Spielerkontos hinzuzufügen; und
- b) bei Abschluss des Bonus/Features alle Geldbeträge auf der temporären „Gewinn“-Anzeige der Guthabenanzeige oder dem Guthaben des Spielerkontos hinzuzufügen.

4.8.4 Gemeinschaftsboni

Gemeinschaftsboni, bei denen Spieler zusammenarbeiten und/oder um eine gemeinsame Prämie spielen, müssen:

- a) eine geeignete Beschreibung der Regeln für jeden Gemeinschaftsbonus, jede Auszahlung und alle Teilnahmebedingungen für den Gewinn von Gemeinschaftsboni enthalten;
- b) kontinuierlich und deutlich sichtbar den Anspruch des Spielers auf einen Gemeinschaftsbonus anzeigen, unabhängig von der Credit-Anzahl im Spiel. Wenn dem Spieler beispielsweise ein dreißigsekündiger Anspruch verbleibt, sein Guthaben jedoch aufgebraucht ist, zeigt das Spiel weiterhin die verbleibenden Sekunden an; und
- c) Benachrichtigung des Spielers bei Gemeinschaftsboni, die nicht von der Anzahl verfügbarer Credits abhängen, über seinen weiterhin bestehenden Anspruch, unabhängig davon, ob sich noch Credits des Spielers im Spiel befinden.

4.8.5 Verdopplungs-/Risiko-Features

Die folgenden Anforderungen gelten für Spiele, die eine Form von Verdopplungs-/Risiko-Feature anbieten. In solchen Spielen kann eine alternative Terminologie zur Beschreibung eines Verdopplungs-/Risiko-Features verwendet werden, wie beispielsweise „Verdreifachung“ oder „Annehmen oder riskieren“:

- a) Alle Anleitungen zu Verdopplungs-/Risiko-Features müssen vollständig in der Spiel-Illustration enthalten sein und ohne Teilnahme an dem Feature zugänglich sein;
- b) der Zugang zu einem Verdopplungs-/Risiko-Feature darf nur nach Abschluss eines primären Spiels möglich sein, in dem ein Gewinn erzielt wurde;
- c) der Spieler muss entscheiden können, ob er an dem Verdopplungs-/Risiko-Feature teilnimmt;
- d) das Verdopplungs-/Risiko-Feature muss eine theoretische Ausschüttungsquote von einhundert Prozent (100 %) aufweisen;
- e) die maximale Anzahl verfügbarer Verdopplungen/Risikospiele muss klar angegeben werden. Alternativ kann dem Spieler das Prämienlimit für Verdopplungen/Risikospiele genannt werden;
- f) es darf nur Guthaben für Einsätze in einem Verdopplungs-/Risiko-Feature zur Verfügung stehen, das im Primärspiel gewonnen wurde (d. h. es ist nicht möglich, jegliche Geldbeträge der Guthabenanzeige oder aus dem Guthaben des Spielerkontos für Verdopplungs-/Risiko-Features zu verwenden);
- g) wenn das Verdopplungs-/Risiko-Feature automatisch abgebrochen wird, bevor die maximale Anzahl verfügbarer Verdopplungen/Risikospiele erreicht ist, muss der Grund deutlich angegeben werden;
- h) jegliche Spielbedingungen, unter denen das Verdopplungs-/Risiko-Feature nicht verfügbar ist, müssen angegeben werden;
- i) wenn ein Verdopplungs-/Risiko-Feature eine Auswahl von Multiplikatoren anbietet, müssen der Auswahlbereich und die Auszahlungen für den Spieler klar erkennbar sein; und
- j) wenn der Spieler einen Multiplikator für ein Verdopplungs-/Risiko-Feature auswählt, muss auf dem Bildschirm klar angegeben werden, welcher Multiplikator ausgewählt wurde.

4.8.6 Mystery-Prämien-Features

Eine Mystery-Prämie ist eine Prämie, die in einem Spiel ausgezahlt wird, das nicht mit speziellen Gewinn Tabellen-Kombinationen verbunden ist. Es ist akzeptabel, wenn innerhalb von Spielen Mystery-Prämien angeboten werden, jedoch müssen in der Spiel-Illustration die Mindest- und Höchstbeträge angegeben sein, die der Spieler potenziell gewinnen kann. Wenn der potenzielle Gewinnbetrag gleich null ist, muss er nicht explizit angezeigt werden. Wenn der Wert der Mystery-Prämie von getätigten Einsätzen oder jeglichen anderen Faktoren abhängt, müssen diese klar angegeben werden.

4.9 Alternative Spielmodi

4.9.1 Freispielmodus

Der Freispielmodus bietet einem Spieler die Möglichkeit, ohne Einsatz an einem Spiel teilzunehmen. Wenn das Spiel einen Betrieb im Freispielmodus unterstützt, müssen folgende Anforderungen erfüllt werden:

- a) Freispiele müssen den normalen Betrieb eines gebührenpflichtigen Spiels präzise abbilden. Im Freispielmodus gespielte Spiele dürfen den Spieler bezüglich der Wahrscheinlichkeit für den Gewinn jeglicher Prämien, die in der Version mit Geldeinsätzen verfügbar sind, nicht in die Irre führen;
- b) der Freispielmodus muss gut sichtbar angezeigt werden, so dass ein Spieler jederzeit weiß, ob/wenn dieser Modus aktiv ist;
- c) der Freispielmodus darf die Guthabenanzeige oder das Kontoguthaben des Spielers nicht erhöhen. Spezielle Anzeigen für diesen Modus sind zulässig, sofern die Anzeigen als solche gekennzeichnet sind;
- d) der Freispielmodus muss beendet werden, wann immer der Spieler sich entscheidet, diesen Modus zu verlassen, oder wenn die Freispiele abgeschlossen sind; und
- e) wenn der Freispielmodus verlassen wird, muss das Spiel in seinen vorherigen Zustand zurückkehren.

HINWEIS: Gebührenpflichtige Spiele, die mit Guthaben aus Anreizprämien gespielt werden, gelten nicht als Freispiele.

4.9.2 Automatischer Spielmodus

Der automatische Spielmodus ermöglicht dem Spiel, ohne Spielerinteraktion automatisch Einsätze zu tätigen, sobald eine Stückelung, ein Einsatz und andere Spielattribute durch den Spieler ausgewählt wurden. Wenn das Spiel einen automatischen Spielmodus unterstützt, gelten die folgenden Regeln:

- a) Der automatische Spielmodus muss sicher mithilfe einer Funktion gesteuert werden, die das Feature entweder zulässt oder verbietet, entsprechend den Präferenzen der jeweiligen Jurisdiktion;
- b) der automatische Spielmodus kann dem Spieler die Möglichkeit bieten, den einzelnen Spieleinsatz, die Anzahl der Einsätze im automatischen Spielmodus und/oder den einzusetzenden Gesamtbetrag auszuwählen;

- i. alle spielerdefinierten Schwellenwerte bleiben für die Dauer des automatischen Spiels wirksam;
 - ii. das Spiel muss die Anzahl der im automatischen Spiel verbleibenden oder verwendeten Einsätze entsprechend eines vom Spieler definierten Schwellenwerts anzeigen;
 - iii. der automatische Spielmodus muss automatisch beendet werden und es muss eine Rückkehr zum manuellen Spielmodus erfolgen, wenn spielerdefinierte Schwellenwerte erreicht werden;
- c) im automatischen Spielmodus muss dem Spieler die Möglichkeit geboten werden, den automatischen Spielmodus nach Abschluss eines aktuellen Spiels zu beenden, unabhängig von der Anzahl der ursprünglich ausgewählten oder der verbleibenden Anzahl von Einsätzen im automatischen Spielmodus; und
- d) wenn Spieleroptionen für den automatischen Modus unterstützt werden, müssen diese Optionen standardmäßig dem manuellen Spielmodus entsprechen.

4.9.3 Turniermodus

Der Turniermodus bietet einem Spieler die Möglichkeit, im Rahmen eines organisierten, überwachten Ereignisses gegen andere Spieler anzutreten. Das Spielen im Turniermodus kann mit oder ohne Geldeinsätze erfolgen. Wenn das Spiel einen bestimmten Turniermodus unterstützt, der sich vom regulären Spielablauf unterscheidet, müssen folgende Anforderungen erfüllt werden:

- a) Alle Regeln im Abschnitt „Wettbewerbe/Turnier“ dieses Dokuments müssen dem Spieler mitgeteilt werden;
- b) der Spieler muss eine Möglichkeit erhalten, sich für oder gegen die Teilnahme zu entscheiden. Bei der Registrierung muss der Spieler die Möglichkeit erhalten, sein Nicht-Turnierspiel vor dem Eintritt in den Turniermodus zu beenden, sofern die Spielplattform nicht die gleichzeitige Teilnahme an Turnierspielen und Nicht-Turnierspielen unterstützt;
- c) im Spiel muss dem Spieler gut sichtbar angezeigt werden, dass sich das Spiel in einem Turniermodus befindet;
- d) bei Turnieren ohne Geldeinsatz darf das Spiel weder Echtgeld aus jeglichen Quellen akzeptieren noch Echtgeld auf jedwede Weise auszahlen. Im Turniermodus müssen turnierspezifische Credits, Punkte oder Chips ohne Geldwert verwendet werden;
- e) bei zeitbasierten Turnieren muss den Spielern ein Timer angezeigt werden, um auf die verbleibende Spieldauer hinzuweisen. Wenn ein Turnier auf einer erweiterten Spieldauer basiert oder bei Eintritt eines bestimmten Ereignisses initiiert oder beendet wird, muss diese Information den Spielern zur Verfügung gestellt werden;
- f) bei Abschluss des Turniers müssen die Spielerplatzierungen angezeigt und der/die Gewinner benachrichtigt werden;
- g) beim Verlassen des Turniermodus muss das Spiel in den ursprünglichen Zustand zurückkehren, in dem es sich vor dem Eintritt in den Turniermodus befand; und
- h) alle für den Spieler im Spiel enthaltenen turnierspezifischen Spielanzeigen müssen beim Verlassen des Turniermodus automatisch gelöscht werden.

4.10 Spiele mit Fähigkeitselementen

4.10.1 Allgemeines

Ein Spiel mit Fähigkeitselementen beinhaltet in seinem Aufbau ein oder mehrere Elemente, die von einem Spieler genutzt werden können, um die Ausschüttungsquote zu verändern. Fähigkeit bezeichnet die menschlichen Attribute eines Spielers wie Kenntnisse, Geschicklichkeit, visuelle Erfassung, Logik, Erinnerungsvermögen, Reaktion, Stärke, Agilität, Sportlichkeit, Hand-Auge-Koordination, numerische und/oder lexikalische Fähigkeiten oder für das Spiel relevante Kompetenzen. Die in diesem Abschnitt definierten Anforderungen gelten für Spiele mit Fähigkeitselementen, um Spieler-Fairness und Klarheit in Bezug auf die Spielerbenachrichtigung sicherzustellen.

HINWEIS: Diese technische Norm soll kein Spiel als „Fähigkeitsspiel“ klassifizieren oder als rechtliche Basis für eine Spielklassifizierung im Zusammenhang mit Fähigkeiten dienen. Solche Klassifizierungen unterliegen der Interpretation durch die Regulierungsbehörde.

4.10.2 Anzeige bei Spielen mit Fähigkeitselementen

Ein Spiel mit Fähigkeitselementen muss den anwendbaren Anzeige-Anforderungen in den entsprechenden Abschnitten „Spielinformationen und Spielregeln“, „Anzuzeigende Informationen“ und „Spiel-Fairness“ dieser Norm entsprechen. Darüber hinaus muss in allen anderen Spielen mit Fähigkeitselementen als den herkömmlichen Casinospiele (z. B. Poker, Blackjack etc.) klar erkennbar darauf hingewiesen werden, dass das Ergebnis durch die Spielerfähigkeiten beeinflusst wird. Diese Information muss deutlich sichtbar angezeigt werden, bevor ein Einsatz getätigt wird.

4.10.3 Virtueller Gegner

In einem Spiel mit Fähigkeitselementen kann einem Spieler die Möglichkeit geboten werden, gegen einen virtuellen Gegner anzutreten, sofern auf der Spielplattform:

- a) klar und deutlich sichtbar darauf hingewiesen wird, wenn ein virtueller Gegner teilnimmt; und
- b) verhindert wird, dass der virtuelle Gegner privilegierte Informationen des Live-Spielers nutzt, anhand derer eine Entscheidung gefällt wird, sofern der Spieler anderslautend informiert wurde.

4.10.4 Ergebnis bei Spielen mit Fähigkeitselementen

Sofern dem Spieler nicht anderslautend mitgeteilt, darf nach der Initiierung eines Spiels mit Fähigkeitselementen keine Spielfunktion in Verbindung mit dem Spielergebnis während des Spiels mehr verändert werden. Darüber hinaus muss dem Spieler bei Änderungen der verfügbaren Gewinntabellen oder Spielregeln zwischen Spielen über die Spiel-Illustration eine deutlich sichtbare Benachrichtigung angezeigt werden. Außerdem müssen angemessene Informationen bereitgestellt werden, damit der Spieler anhand dieser eine Entscheidung treffen kann. Ein Beispiel für den letzteren Fall kann eine Kennung sein, die genutzt wird, um die verfügbaren Gewinntabellen während des Spielverlaufs zu ändern.

4.10.5 Wahrscheinlichkeiten für fähigkeitsbasierte Prämien

Wenn die höchste angegebene Prämie fähigkeitsbasiert ist, muss sie von einem Spieler erreicht werden können. Wenn diese fähigkeitsbasierte Prämie ein Glückselement beinhaltet, muss die Möglichkeit, die Prämie zu erhalten den bereits zuvor in diesem Dokument dargelegten Anforderungen für „Wahrscheinlichkeiten“ entsprechen.

4.10.6 Beratungsfunktionen für Spieler

Ein Spiel mit Fähigkeitselementen kann eine Funktion unterstützen, die einem Spieler Ratschläge, Hinweise oder Vorschläge bietet. Ein veranschaulichendes Beispiel kann ein Wissensspiel sein, in dem Spieler Hinweise, Spuren oder andere Hilfestellungen bei einer Auswahl erhalten. Ein Spiel mit Fähigkeitselementen kann Beratungsfunktionen für Spieler unterstützen, sofern es die folgenden Anforderungen erfüllt:

- a) Die Beratungsfunktion für Spieler muss den Spieler klar darauf hinweisen, dass sie verfügbar ist und welche Wahlmöglichkeiten bestehen;
- b) bei allen kostenpflichtigen Ratschläge zum Spiel, die dem Spieler angeboten werden, müssen die Kosten und der Nutzen klar dargelegt werden;
- c) der Ratschlag für den Spieler darf nicht missverständlich oder unpräzise sein und muss den Spielregeln entsprechen, während gleichzeitig darauf hingewiesen wird, dass die Spielregeln in Abhängigkeit vom angebotenen Ratschlag geändert werden können, wobei dem Spieler alle derartigen Änderungen vor der Annahme des Ratschlags mitgeteilt werden;
- d) der Spielaufbau muss den Zugriff auf jegliche „Informationsspeicher“ derart verhindern, dass Daten in Verbindung mit dem Fähigkeitselement durch Software-Manipulation nicht direkt verfügbar sind (beispielsweise muss bei einem Wissensspiel der Zugriff auf die Antwort-Datenbank verhindert werden);
- e) die Spielerberatungs-Funktion muss dem Spieler die Möglichkeit bieten, den Ratschlag anzunehmen und darf den Spieler nicht zwingen, die Hilfestellung zu akzeptieren, sofern sie zu diesem Zeitpunkt für den Spieler nicht die einzig mögliche Option darstellt, das Spiel fortzusetzen; und
- f) die Verfügbarkeit und die Inhalte der Spielerberatung müssen konsistent bleiben, sofern nicht anders angegeben, und es dürfen keine Anpassungen vorgenommen werden, die den Spieler basierend auf vorherigen Spielen oder Spielereignissen benachteiligen.

HINWEIS: Es wird empfohlen, dass die Spielplattform eine sichere Möglichkeit unterstützt, die Spielerberatung zu aktivieren oder zu deaktivieren, um die Vorgaben von Regulierungsbehörden zu erfüllen, die diese Art von Funktion entweder gestatten oder verbieten können.

4.10.7 Für Spiele mit Fähigkeitselementen genutzte Spieler-Interaktionsgeräte

Wenn eindeutige Spieler-Interaktionsgeräte (z. B. Joysticks, Spiel-Controller, Kamerasysteme, Soundsysteme, Bewegungssensoren, Beschleunigungsmesser etc.) innerhalb des Spiels genutzt werden, um Fähigkeiten zu unterstützen, muss das Spiel mit Fähigkeitselementen adäquate und eindeutige Anweisungen in Bezug auf ihren Zweck, die Nutzung und die Wirkung bereitstellen. Wenn sich mehrere Spieler-Interaktionsgeräte auf dieselbe Spielerhandlung, die Fähigkeitselemente beinhalten, auswirken, müssen dem Spieler alle derartigen Optionen deutlich erklärt werden.

4.11 Peer-to-Peer (P2P)-Spiele

4.11.1 P2P-Spielsitzungen

Peer-to-Peer (P2P)-Spielsitzungen sind Umgebungen, die Spielern die Möglichkeit bieten, mit- und gegeneinander zu spielen. In diesen Umgebungen ist der Betreiber üblicherweise nicht als Partei an den P2P-Spielsitzungen beteiligt, stellt aber die Umgebung bereit, die von seinen Spielern genutzt werden kann, und er kann für den Service ein Rake, eine Provision oder eine Gebühr in Rechnung stellen. Es gelten die folgenden Anforderungen:

- a) Die Spieler müssen daran gehindert werden, mehr als eine Position in einer beliebigen P2P-Spielsitzung zu belegen, sofern dies nicht durch die Spielregeln autorisiert ist;
- b) die Spieler müssen über die Möglichkeit verfügen, einer P2P-Spielsitzung beizutreten, in der alle Spieler zufällig ausgewählt wurden;
- c) alle Spieler, die mit Hausgeld (Shills) spielen oder Proposition-Spieler müssen für alle anderen Spieler in dieser P2P-Sitzung klar erkennbar sein; und
- d) die Spieler müssen gewarnt werden, wenn Bots oder andere nicht autorisierte Spieler-Software das Spiel beeinflussen können, so dass sie in der Lage sind, eine informationsbasierte Entscheidung zu treffen, ob sie teilnehmen möchten.

4.11.2 P2P-Vorteilsfunktion

Eine P2P-Spielsitzung kann eine Funktion umfassen, die es einem oder mehreren Spielern ermöglicht, einen Vorteil gegenüber anderen Spielern zu erlangen, vorausgesetzt, das Spiel:

- a) weist alle Spieler deutlich darauf hin, dass die Funktion verfügbar ist und welchen Vorteil sie bietet;
- b) legt die Methode für die Nutzung der Funktion offen, einschließlich aller erforderlichen Einsätze; und
- c) liefert Spielern ausreichende Informationen, um vor dem Spiel eine fundierte Entscheidung zu treffen, ob sie gegen andere Spieler antreten möchten, die möglicherweise über eine solche Funktion verfügen.

4.11.3 „Abwesenheits“-Status

Die Spielplattform muss einen „Abwesenheits“-Status unterstützen, der entweder auf Spielieranforderung oder nach einer Zeitspanne der Inaktivität ausgelöst wird. Die Dauer muss dem Spieler mitgeteilt werden und maximal der im Abschnitt „Spieler-Inaktivität“ dieses Dokuments angegebenen Inaktivitäts-Zeitspanne entsprechen. Dieser Status muss vollständig auf den Hilfebildschirmen oder in den anwendbaren Spielregeln beschrieben werden.

- a) Der Spieler muss informiert werden, wenn der „Abwesenheits“-Status aktiviert wird.
- b) Der „Abwesenheits“-Status muss alle Spielaktivitäten unterbinden und den Spieler automatisch in jeder stattfindenden Spielrunde überspringen, während dieser Status aktiv ist.
- c) Wenn der „Abwesenheits“-Status in der Mitte eines Spiels aktiviert wird, muss dieses Spiel als unterbrochenes Spiel behandelt werden und die Anforderungen im Abschnitt „Abschließen

- unterbrochener Spiele“ erfüllen.
- d) Wenn ein Spieler im „Abwesenheits“-Status eine spielsensible Handlung durchführt (z. B. Auswahl eines Einsatzbetrages etc.), muss der Status entfernt werden und der Spieler wird für das nächste Spiel angemeldet. Nicht spielsensible Aktionen wie der Zugriff auf das Hilfemenü erfordern kein Entfernen dieses Status.
 - e) Wenn sich ein Spieler über einen längeren, ihm bekannt gegebenen Zeitraum hinweg im „Abwesenheits“-Status befindet, muss er automatisch aus der P2P-Spielsitzung entfernt werden, an der er aktuell teilnimmt.

4.12 Persistenz-Spiele

4.12.1 Allgemeines

Ein Persistenz-Spiel ist mit einem eindeutigen Attribut verknüpft (z. B. Spieler-ID, Spielthema-/Gewinntabellen- ID etc.) und umfasst eine Funktion zur Fortschrittsverfolgung für Spielverbesserungen und/oder Boni durch das Erreichen einiger bestimmter Spielergebnisse. Diese zusätzlichen Angebote sind verfügbar, wenn der Spieler bestimmte für das Spiel definierte Schwellenwerte erreicht hat. Jedes bestimmte Ergebnis verbessert den Status des Persistenz-Spiels. Üblicherweise muss ein Spiel mehrfach gespielt werden, um die Persistenz-Prämie auszulösen.

4.12.2 Schwellenwerte für Persistenz-Spiele

Ein Persistenz-Spiel muss ein bestimmtes Attribut zur Wiederherstellung zuvor erreichter Schwellenwerte während aller Folgebesuche eines Spiels betrachten. Ein Persistenz-Spiel muss auf seinen Hilfe-Bildschirmen eine klare Beschreibung aller mit Persistenz-Spielen in Verbindung stehenden Features und/oder Funktionen sowie die Anforderungen für das Erreichen von Persistenz-Spiel-Schwellenwerten und Informationen darüber enthalten, wie der Spieler zuvor erreichte Schwellenwerte wiederherstellt. Darüber hinaus müssen die Spieler stets informiert werden, wenn ein Persistenz-Spiel-Schwellenwert erreicht wurde.

4.12.3 Gespeicherte Spielstände spielen

Das Spielen gespeicherter Spielstände ist eine Funktion, die in manchen Persistenz-Spiel-Konzepten genutzt wird, in denen die Komplexität zunimmt oder dem Spiel im weiteren Verlauf zusätzliche Elemente hinzugefügt werden. Darüber hinaus ermöglicht das Spielen gespeicherter Spielstände dem Spieler das Speichern eines Persistenz-Spiels an kritischen Punkten (d. h. Speicherpunkten), üblicherweise nach Erreichen eines Erfolgs oder Ziels. Der Spieler kann das Spiel ab diesem Punkt später fortsetzen, um das nächste Ziel zu erreichen. Für das Spielen gespeicherter Spielstände gelten die folgenden Anforderungen:

- a) Prämien, die für das Erreichen eines Speicherpunktes vergeben oder zur Verfügung gestellt werden, müssen klar definiert und dem Spieler angezeigt werden, bevor jegliche Einsätze getätigt werden. Wenn eine Zufallsprämie gewonnen werden kann, müssen dem Spieler die Details und sämtliche möglichen Auszahlungen angezeigt werden;
- b) das Spiel muss den Spieler in geeigneter Weise benachrichtigen, wenn während des Spiels ein bestimmter Speicherpunkt erreicht wird;

- c) wenn sich während des Spielens gespeicherter Spielstände mit dem Erreichen verschiedener Stufen Spielregeln oder Prämien ändern, müssen diese Änderungen dem Spieler deutlich angezeigt werden; und
- d) wenn das Spielen gespeicherter Spielstände nicht auf unbestimmte Zeit möglich ist, muss das Spiel den Spieler über jegliche Einschränkungen und/oder Gültigkeitszeiträume gespeicherter Daten informieren, die dem Fortsetzen des Spiels zu einem späteren Zeitpunkt dienen.

4.13 Progressive Jackpots und stufenweise Jackpots

4.13.1 Allgemeines

Dieser Abschnitt gilt für monetäre Jackpot-Prämien oder „Auszahlungen“, die basierend auf dem Spielverlauf wie folgt ansteigen:

- a) Progressive Jackpot-Prämien werden den im Spiel eingesetzten Credits entsprechend erhöht.
- b) Das Verhalten bei Prämien von stufenweisen Jackpots ist identisch zu dem bei progressiven Jackpots, außer dass ihre Erhöhung basierend auf einer oder mehreren bestimmten Bedingungen (definierte Ereignisse) erfolgt, die in den Spielregeln festgelegt sind, statt oder zusätzlich zu Erhöhungen, die auf eingesetztem Guthaben basieren.

HINWEIS: Dieser Abschnitt gilt nicht für restriktive Anreizgutschriften, Boni/Features, die Preise bieten, welche innerhalb eines einzelnen Spielzyklus erhöht werden, oder statische Preise, deren Auslösungswahrscheinlichkeiten sich im Spielverlauf ändern. Dieser Abschnitt gilt ebenfalls nicht für Persistenz-Spiel-Features, bei denen die Erhöhung während des Spielverlaufs erfolgt (z. B. Anzahl von Freispielen, Multiplikatoren, mehrere erreichte Ziele zur Aktivierung eines Bonus/Features oder der Vergabe einer Prämie etc.) oder „Stufen“ verfügbarer statischer Prämien, die basierend auf der Spielererfahrung und/oder Erfolgen gewonnen werden.

4.13.2 Jackpot-Anzeige

Die Jackpot-Anzeige wird verwendet, um den aktuellen Jackpot-Gewinnbetrag oder die „Auszahlung“ für jeden Jackpot in Credits oder im lokalen Währungsformat für alle Spieler darzustellen, die an einem Spiel teilnehmen, das potenziell den Jackpot auslösen kann. Wenn der Jackpot eine „Mystery-Auszahlung“ bietet, bei der der tatsächliche Auszahlungsbetrag dem Spieler nicht angezeigt wird, finden die „Mystery-Prämien-Features“ Anwendung.

- a) Während der Teilnahme an Spielen muss die aktuelle Auszahlung für jeden Jackpot auf der Jackpot-Anzeige mindestens alle dreißig Sekunden durch das erhöhende Spielereignis aktualisiert werden, um die tatsächliche Auszahlungshöhe widerzuspiegeln. Die Nutzung von Wegmessern und anderen „geschwindigkeitsbasierten“ aktualisierenden Anzeigen ist zulässig.
- b) Wenn die Jackpot-Anzeige eine maximale Anzeigebegrenzung aufweist (d. h. nur eine bestimmte Anzahl von Stellen darstellen kann), ist ein maximales Auszahlungslimit oder eine „Deckelung“ erforderlich, welche die Anforderungen für „Maximale Auszahlungslimits“ erfüllt.

HINWEIS: Die Auszahlung(en) muss/müssen innerhalb der Einschränkungen durch Kommunikationsverzögerungen und Latenzen so präzise wie möglich angezeigt werden.

4.13.3 Maximale Auszahlungslimits

Wenn ein maximales Auszahlungslimit oder eine „Deckelung“ vom Jackpot unterstützt wird, bleibt ihr Wert nach Erreichen der Deckelung bestehen, bis eine Vergabe an den Spieler erfolgt.

- a) Wo von der Regulierungsbehörde gefordert, müssen alle zusätzlichen Beiträge einem Überlauf- oder Umleitungspool gutgeschrieben werden.
- b) Dem Spieler in der Illustration bekannt gegebene Deckelungsbeträge müssen präzise sein.

4.13.4 Verknüpfte Wahrscheinlichkeiten

Bei Jackpots, die mit mehreren Spielthemen verknüpft sind, muss sich die Wahrscheinlichkeit auf den Gewinn des verknüpften Jackpots proportional zum Geldeinsatz des Spielers verhalten, sofern dem Spieler nicht anderslautend mitgeteilt.

HINWEIS: Für die Zwecke dieser Anforderung ist eine Varianz von maximal fünf Prozent (5 %) für die Wahrscheinlichkeit und maximal einem Prozent (1 %) Toleranz bei der Berechnung der erwarteten RTP akzeptabel.

4.13.5 Jackpot-Umleitung

Wenn von der Regulierungsbehörde gestattet, kann ein Jackpot-Umleitungsschema verwendet werden, bei dem ein Teil der Jackpot-Beiträge in einen anderen Pool oder „Umleitungspool“ überführt werden, um je nach Bedarf des Jackpot-Spiels verwendet zu werden (z. B. kann der Umleitungspool dem Resetwert des nächsten Jackpots hinzugefügt oder zur Auszahlung gleichzeitiger Gewinne eines Jackpots genutzt werden).

- a) Ein Jackpot-Umleitungsschema muss so implementierbar sein, dass es keinen unendlichen mathematischen Erwartungswert aufweist.
- b) Umleitungspools dürfen nicht gekürzt werden. Sobald dieser Umleitungspool seine Obergrenze erreicht hat, müssen umgeleitete Beiträge abgerechnet werden.
- c) Wenn ein Umleitungspool genutzt wird, um den Resetwert eines Jackpots zu finanzieren, muss der Resetwert für RTP-Berechnungen von einem leeren Umleitungspool ausgehen.

4.13.6 Jackpot-Gewinne

Jackpots können basierend auf erhaltenen Gewinnsymbolen oder aufgrund anderer Kriterien gewonnen werden, wie beispielsweise einer Mystery-Auslösung, Bad-Beat-Jackpots etc. Wenn ein Jackpot ausgelöst wird:

- a) Ein Gewinner muss am Ende des laufenden Spiels über den Jackpot-Gewinn und seine Auszahlung benachrichtigt werden.
- b) Beiträge zum Jackpot dürfen nicht verloren werden. Zuerkannte Jackpot-Auszahlungen dürfen nicht abgerundet oder gekürzt werden, sofern kein Übertrag auf den Resetbetrag erfolgt.
- c) Bei Verwendung kann die Jackpot-Auszahlung der Guthabenanzeige des Spielers hinzugefügt werden, wenn entweder:

- i. die Guthabenanzeige im lokalen Währungsformat geführt wird;
 - ii. die Jackpot-Auszahlung in ganzzahligen Credit-Beträgen erhöht wird; oder
 - iii. die Jackpot-Auszahlung im lokalen Währungsformat bei der Übertragung auf die Guthabenanzeige auf eine den Spieler nicht irreführende Weise korrekt in Credits umgerechnet wird.
- d) Die Jackpot-Auszahlung muss auf den Resetwert aktualisiert und der Normalbetrieb fortgesetzt werden.

HINWEIS: Ein Jackpot kann mit dem Gewinn des Jackpots deaktiviert oder außer Kraft gesetzt werden, wenn das Spiel so konfiguriert wurde, dass eine automatische Deaktivierung erfolgt oder eine sich nicht erhöhende Prämie eingesetzt wird.

4.13.7 Wechsel zwischen Jackpot-Stufen

Bei Jackpots mit mehreren Gewinnstufen muss, wenn eine einzelne Gewinnkombination für mehr als eine der verfügbaren Gewinn Tabellen-Kombinationen gewertet werden kann, sofern nicht in den Spielregeln anders definiert, der Spieler stets den größtmöglichen Wert basierend auf allen Kombinationen erhalten, mit denen das Ergebnis zusammenhängt (z. B. wenn „Jackpot A“ für fünf Asse auf einer Gewinnlinie und „Jackpot B“ für vier Asse auf einer Gewinnlinie vergeben wird, wobei „Jackpot B“ einen größeren Gewinn darstellt als „Jackpot A“, muss der Spieler die Auszahlung für „Jackpot B“ erhalten, wenn der Spieler als Ergebnis fünf Asse auf einer Gewinnlinie erhält).

4.13.8 Jackpots mit Mystery-Auslösung

Bei Jackpots mit Mystery-Auslösung, die einen verborgenen Auslösungsbetrag nutzen, um den Zeitpunkt des Jackpot-Gewinns zu bestimmen:

- a) Der verborgene Auslösungsbetrag muss bei jedem Zurücksetzen des Jackpots zufällig bestimmt werden und zu jeder Zeit unbekannt bleiben; und
- b) es darf zu keinem Zeitpunkt möglich sein, auf den verborgenen Auslösungsbetrag zuzugreifen oder Kenntnis über diesen zu erlangen.

4.13.9 Jackpot-Auslösungen für mehrere Spieler

Die Spielplattform muss so gestaltet sein, dass die Reihenfolge der Auslöser bei einem nahezu gleichzeitigen Auslösen durch mehrere Spieler präzise erkannt und aufgezeichnet wird, so dass der vollständige Betrag der angezeigten Auszahlung an den zuerst auslösenden Gewinner vergeben werden kann. Wenn dies nicht möglich ist oder die Möglichkeit besteht, dass mehrere Spieler genau zur selben Zeit auslösen (z. B. in einem Multiplayer-Spiel) muss eine der folgenden Maßnahmen ergriffen werden:

- a) Der vollständige Betrag der angezeigten Auszahlung muss jedem Gewinner zuerkannt werden; oder
- b) der Spieler muss genaue Informationen über die Aufteilung der Auszahlung erhalten.

4.14 Spielrekonstruktion

4.14.1 Spielerseitige Spielrekonstruktion

Dem Spieler muss eine Möglichkeit zur „Spielrekonstruktion“ geboten werden, entweder in Form einer Nachstellung oder einer Beschreibung. In der Spielrekonstruktion muss klar darauf hingewiesen werden, dass es sich um eine Wiederholung des vorherigen Spielverlaufs handelt.

4.14.2 Informationen zum letzten Spiel erforderlich

Die Spielrekonstruktion muss aus Grafik-, Text oder Videoinhalten oder einer Kombination aus diesen oder anderen Hilfsmitteln bestehen (z. B. „Flugschreiber“-Mechanismus), solange die vollständige und präzise Rekonstruktion des Spielverlaufs und/oder der Spieleraktionen möglich ist. Es ist zulässig, Werte anstelle von Credits in einem Währungsformat anzuzeigen. Die Spielrekonstruktion muss die folgenden Informationen wiedergeben, sofern anwendbar:

- a) das Datum und die Uhrzeit, zu der das Spiel gespielt wurde;
- b) die für das Spiel gespielte Stückelung, sofern es sich um einen Spieltyp mit Mehrfach-Stückelung handelt;
- c) die mit dem Endergebnis des Spiels verbundene Anzeige, entweder grafisch oder mit einer klaren Textbeschreibung;
- d) die zu Beginn und/oder am Ende des Spiels als Einsatz verfügbaren Geldbeträge;
- e) den eingesetzten Gesamtbetrag, einschließlich jeglicher Anreizgutschriften;
- f) den gewonnenen Gesamtbetrag, einschließlich:
 - i. jeglicher Anreizgutschriften und/oder Preise;
 - ii. alle progressiven Jackpots und/oder stufenweisen Jackpots;
- g) alle nicht einsatzbezogenen Käufe zwischen dem Beginn und dem Ende des Spiels;
- h) in Rechnung gestellte Rakes, Provisionen oder Gebühren;
- i) die Ergebnisse aller anderen am Spielergebnis beteiligten Spielerentscheidungen;
- j) die Ergebnisse aller Übergangs-Spielphasen wie Verdopplungs/Risiko- oder Bonus-/Feature-Spiele;
- k) wenn ein progressiver Jackpot oder ein stufenweiser Jackpot gewonnen wurde, einen Hinweis, dass der Jackpot vergeben wurde; und
- l) alle Ratschläge zum Spiel, die dem Spieler für Spiele mit Fähigkeitselementen angeboten wurden.

4.14.3 Rekonstruktion von Bonus-/Feature-Spielen

Das Spiel muss mindestens die letzten fünfzig Ereignisse abgeschlossener Bonus-/Feature-Spiele widerspiegeln. Wenn ein Bonus-/Feature-Spiel aus „x Ereignissen“ mit jeweils separaten Ergebnissen besteht, muss jedes der „x Ereignisse“ (bis zu fünfzig) mit seinem entsprechenden Ergebnis angezeigt werden, unabhängig davon, ob das Ergebnis ein Gewinn oder ein Verlust war.

4.15 Deaktivierungs-Anforderungen

4.15.1 Spiel-Deaktivierung

Wenn ein Spiel oder eine Spielaktivität während eines laufenden Spiels durch die Spielplattform deaktiviert wird, muss allen an diesem Spiel teilnehmenden Spielern gestattet werden, ihr aktuelles Spiel zu beenden (d. h. Bonusrunden, Verdopplungen/Risikospiele und andere Spiel-Features in Verbindung mit dem Einsatz müssen sofort oder beim nächsten Mal, wenn das Spiel für den Spieler verfügbar ist, vollständig abgeschlossen werden). Nachdem das Spiel vollständig abgeschlossen ist, darf es für einen Spieler nicht mehr zugänglich sein.

4.15.2 Jackpot-Deaktivierung

In Fällen, in denen ein progressiver Jackpot oder ein stufenweiser Jackpot deaktiviert wird (z. B. Eingreifen des Betreibers, Fehlerzustand, abgelaufenes Zeitlimit etc.) gelten die folgenden Anforderungen:

- a) Ein Hinweis muss angezeigt werden, wenn der Jackpot nicht verfügbar ist;
- b) es darf nicht möglich sein, den Jackpot in diesem Status zu erhöhen oder zu gewinnen; und
- c) bei der Rückführung des Jackpots aus dem deaktivierten Zustand muss die Möglichkeit bestehen, den Jackpot mit denselben Parametern zu reaktivieren wie vor der Deaktivierung, einschließlich der Auszahlung. Der verborgene Auslösungsbetrag, sofern zur Bestimmung des Jackpot-Gewinns für einen Jackpot mit Mystery-Auslösung genutzt, kann nur erneut ausgewählt werden, wenn der erneut gewählte Betrag im Bereich zwischen aktueller Auszahlung und Deckelung liegt.

HINWEIS: Bei Hausbank-Spielen wird empfohlen, dass bei Nichterfüllen der prozentualen Mindestanforderung gemäß Abschnitt „Software-Anforderungen für prozentuale Auszahlungen“, wenn der Jackpot nicht verfügbar ist, die beteiligten Spiele ebenfalls deaktiviert werden.

4.16 Unterbrochene Spiele

4.16.1 Unterbrochene Spiele

Ein Spiel gilt als unterbrochen, wenn das Spielergebnis ausstehend bleibt oder das Ergebnis dem Spieler nicht korrekt vermittelt werden kann. Unterbrochene Spiele können aus folgenden Ereignissen während des Spiels resultieren:

- a) Verlust der Kommunikation zwischen der Spielplattform und dem Remote-Spieler-Gerät;
- b) Neustart der Spielplattform;
- c) Neustart oder Fehlfunktion eines Remote-Spieler-Geräts;
- d) unnormales Beenden der Spieler-Software; oder
- e) Befehl zur Spiel-Deaktivierung durch die Spielplattform.

4.16.2 Einsätze in unterbrochenen Spielen

Einsätze in Verbindung mit einem unterbrochenen Spiel, das fortgesetzt werden kann, müssen bis zum Abschluss des Spiels von der Spielplattform gehalten werden. Die Spielerkonten müssen alle Geldbeträge widerspiegeln, die sich in unterbrochenen Spielen befinden.

4.16.3 Abschließen unterbrochener Spiele

Die Spielplattform muss einem Spieler einen Mechanismus bereitstellen, um ein unterbrochenes Spiel abzuschließen. Ein unterbrochenes Spiel muss abgerechnet werden, bevor einem Spieler gestattet wird, in einer anderen Instanz am gleichen Spiel teilzunehmen.

- a) Wenn kein Input durch den Spieler erforderlich ist, um das Spiel abzuschließen, ist es akzeptabel, wenn das Spiel in einen Spielabschluss-Status zurückkehrt, sofern der Spielverlauf und die Guthabenanzeige oder der Stand des Spielerkontos ein abgeschlossenes Spiel widerspiegeln.
- b) Für Einzelspieler-Spiele, in denen ein Input durch den Spieler erforderlich ist, um das Spiel abzuschließen, muss das Spiel den Spieler zurück zu dem Spielstatus unmittelbar vor der Unterbrechung bringen und ihm ermöglichen, das Spiel abzuschließen, sofern dem Spieler keine anderslautenden übergeordneten Spielregeln und/oder Geschäftsbedingungen mitgeteilt wurden.
- c) Wenn bei Multiplayer-Spielen ein Input durch den Spieler erforderlich ist, um das Spiel abzuschließen und der Spieler eine von ihm verlangte Aktion nicht innerhalb der vorgegebenen Zeit durchführen kann, um das Spiel fortzusetzen:
 - i. muss die Spielplattform das Spiel gemäß den Spielregeln und/oder Geschäftsbedingungen für den Spieler abschließen;
 - ii. der Spielverlauf und die Guthabenanzeigen oder Kontostände des Spielers müssen entsprechend aktualisiert werden;
 - iii. die Spielergebnisse müssen dem Spieler zur Verfügung stehen und Angaben enthalten, welche Entscheidungen, sofern zutreffend, für den Spieler durch die Spielplattform getroffen wurden; und
 - iv. die Spielplattform muss so gestaltet sein, dass sich eine nicht innerhalb der vorgegebenen Zeit durchgeführte Aktion eines Spielers hinsichtlich des Spielabschlusses sowie der Abrechnung von Gewinnen oder Verlusten nicht auf andere Spieler in derselben Spielsitzung auswirkt.

4.17 Wetten auf virtuelle Ereignisse

4.17.1 Allgemeines

Das Wetten auf virtuelle Ereignisse ermöglicht die Platzierung von Wetten auf Simulationen von Sportereignissen, Wettbewerben und Rennen, deren Ergebnisse mit Zustimmung der Regulierungsbehörde ausschließlich durch einen genehmigten Zufallszahlengenerator (RNG) bestimmt werden. Spielplattformen, die das Wetten auf virtuelle Ereignisse unterstützen, müssen die Anforderungen für „Wetten auf virtuelle Ereignisse“ in den *GLI-33 Normen für Ereignis-Wettsysteme* erfüllen. Darüber hinaus muss der für Wetten auf virtuelle Ereignisse eingesetzte RNG die anwendbaren „Anforderungen an Zufallszahlengeneratoren (RNG)“ in diesem Dokument erfüllen.

4.18 Live-Spiel-Anforderungen

4.18.1 Allgemeines

Sofern durch eine Regulierungsbehörde autorisiert, gelten die folgenden Anforderungen, wenn über

eine Spielplattform Einsätze in Live-Spielen getätigt werden, die von einem Spielbeteiligten durchgeführt werden (z. B. Kartengeber oder Croupier etc.) und/oder durch andere Spielgeräte (z. B. automatischer Roulettekessel, Kugelgebläse, Spielvorrichtung etc.) in einer Live-Umgebung abgewickelt werden. Dies beinhaltet unter anderem Live-Ziehungen, Live-Kartenspiele, Live-Tischspiele, Live-Keno-Spiele, Live-Bingo-Spiele und Live-Spiele von Spielvorrichtungen oder andere von der Regulierungsbehörde genehmigte Spiele.

- a) Der gesamte Prozess wird von allen Spielern über Remote-Audio- und Videoübertragungen verfolgt, die Streaming, Narrowcasting, Broadcast oder andere Technologien und eine Grafikschnittstelle nutzen.
- b) Die Spielplattform erhält über die Spielerschnittstelle oder einen anderen Kommunikationskanal Anweisungen von jedem Spieler, um bei Bedarf Spielerentscheidungen zu ermöglichen.
- c) Neben den in diesem Abschnitt enthaltenen Anforderungen muss der Betreiber oder der für die Pflege dieser Komponenten, Services und/oder Anwendungen zuständige Drittanbieter den im Abschnitt „Live-Spiel-Services“ dieses Dokuments angegebenen betrieblichen Verfahrensweisen und Kontrollen entsprechen.

HINWEIS: Sofern von einer Regulierungsbehörde autorisiert, kann ein Anbieter von Live-Spiel-Services eine Ersatzvorrichtung nutzen, um Einsätze für einen Spieler zu tätigen, statt direkt über ein System. Solche Implementierungen werden bei Verwendung in Kombination mit einer Spielplattform auf fallweiser Basis geprüft.

4.18.2 Live-Spiel-Informationen

Ein Live-Spiel muss den anwendbaren Anzeige-Anforderungen in den entsprechenden Abschnitten „Spielinformationen und Spielregeln“, „Anzuzeigende Informationen“ und „Spiel-Fairness“ dieser Norm entsprechen. Darüber hinaus gelten die folgenden Anzeige-Anforderungen:

- a) Die Spielplattform muss dem Spieler Informationen bereitstellen, die:
 - i. Implementierte Verfahrensweisen für den Umgang mit Live-Spiel-Unterbrechungen beschreiben, die während eines Spiels durch eine Unterbrechung von Datenfluss, Video und Sprache vom Netzwerkserver verursacht wurden (z. B. Ausfall der Internet-Verbindung, Fehlfunktion des Simulcast-Kontrollservers etc.);
 - ii. auf die Möglichkeit eines menschlichen Fehlers durch den Spielbeteiligten und eines Systemfehlers durch das Spezialgerät hinweisen und erklären, wie Probleme gelöst werden können; und
 - iii. jeden Zusammenhang zwischen der Einsatzauswahl des Spielers über die Spielplattform und der Anzeige im Video-Feed aufzeigt, wie beispielsweise physische Spielerchips und ihr Wert.
- b) Die Spielplattform darf keinerlei Echtzeit-Informationen für das aktuelle gespielte Live-Spiel bereitstellen, die für Folgendes genutzt werden können:
 - i. Vorhersage des Ergebnisses eines Spiels;
 - ii. bei Kartenspielen Verfolgung der gespielten Karten und der noch zu spielenden Karten;
 - iii. Analyse der Wahrscheinlichkeit des Auftretens eines Ereignisses im Zusammenhang mit einem Spiel; oder
 - iv. Analyse der Spiel- oder Einsatzstrategie, die in einem Spiel verwendet werden soll, es sei denn, dies ist nach den Spielregeln zulässig.

- c) Die Spieler müssen bei allen Live-Spielen, die eine „Live“-Überwachung eines Ereignisses nutzen (z. B. Bingo), darüber informiert werden, dass „Live“-Übertragungen Verzögerungen und Unterbrechungen unterliegen können. Wenn eine Verzögerung auftritt oder durch die Spielplattform erzeugt wird, muss dem Spieler der Umfang der Verzögerung angezeigt werden.

4.18.3 Spieler-Fairness in Live-Spielen

Die folgenden Regeln gelten, wenn Spieler über die Spielplattform an Spielen mit persönlich erscheinenden Spielern teilnehmen, die an einem Veranstaltungsort am tatsächlichen Spiel teilnehmen (z. B. Casino, Bingo-Saal, Kartenzimmer etc.):

- a) Die Regeln, Illustrationen und Funktionalitäten des Live-Spiels, die dem Spieler über die Spielplattform zur Verfügung gestellt werden, dürfen nicht mehr oder weniger Informationen beinhalten als einem persönlich teilnehmenden Spieler bereitgestellt würden, sofern anwendbar; und
- b) Spieler, die über eine Spielplattform spielen, müssen im gleichen Umfang gewinnberechtigt sein wie persönlich teilnehmende Spieler.

HINWEIS: Nichts in diesem Dokument schließt die Möglichkeit aus, spezielle Anreizprämien für persönlich oder über eine Spielplattform teilnehmende Spieler zu implementieren.

4.18.4 Spielergebnisdaten

Spielergebnisdaten sind alle Ergebnisse, die während des Live-Spiels von speziellen Vorrichtungen generiert oder erkannt werden, bis einschließlich des Ergebnisses des Spielereinsatzes, inklusive jeglicher Übergangsphasen, die sich auf das von der Spielerplattform bestimmte Ergebnis auswirken. Spielergebnisdaten müssen im Anschluss an ihre Erzeugung oder Erkennung unverzüglich an den Spieler übertragen werden (vorbehaltlich der natürlichen Einschränkungen durch Verzögerungen bei der Systemverarbeitung und der Internet-Kommunikation. Wenn von der Regulierungsbehörde gestattet, können Spielergebnisdaten automatisch durch spezielle Geräte registriert werden, sofern die Software für die automatische Erkennung:

- a) Ein hohes Maß an Genauigkeit bei der Bestimmung und Meldung der Spielergebnisdaten an die Spielplattform gewährleistet. Die Spielregeln müssen in die Spielplattform einprogrammiert werden;
- b) keinerlei Informationen liefert, die zur Kompromittierung des Geräts und seiner Komponenten genutzt werden können (z. B. Karten in der aktuellen Zuteilung oder im Kartenschlitten);
- c) das Verhalten des Geräts nicht stört oder über die mit dieser Software verbundene Funktionalität hinaus verändert; und
- d) einen manuellen Betriebsmodus beinhaltet, um Korrekturen fehlerhafter Ergebnisse zu ermöglichen (wenn das Gerät eine Karte oder die Position der Kugel falsch erkennt etc.), sofern solche Korrekturen nicht direkt auf der Spielplattform erfolgen. Der Spieler muss darauf aufmerksam gemacht werden, dass der manuelle Betriebsmodus verwendet wird.

4.18.5 Physische Zufallsgeräte

In Live-Spielen können physische Zufallsgeräte genutzt werden, um Spielergebnisse zu erzeugen, wie im Abschnitt „Mechanischer RNG (physisches Zufallsgerät)“ dieses Dokuments beschrieben.

- a) Die Ergebnisse physischer Zufallsgeräte müssen zu Spielergebnisdaten digitalisiert und über spezielle Geräte für die Verarbeitung ohne Änderungen an die Spielplattform übertragen werden, sofern nicht anderslautende Genehmigungen der Regulierungsbehörde vorliegen.
- b) Spielergebnisdaten müssen im Anschluss an ihre Erzeugung oder Erkennung unverzüglich von der Spielplattform aufgezeichnet und an dem Spieler zur Verfügung gestellt werden (vorbehaltlich der natürlichen Einschränkungen durch Verzögerungen bei der Systemverarbeitung und der Netzwerk-Kommunikation).
- c) Mit Ausnahme menschlicher Fehler oder durch manuelles Außerkraftsetzen korrigierbarer Fehler müssen die Spielergebnisdaten zu jedem Zeitpunkt während des Spiels mit dem durch das physische Zufallsgerät generierten Ergebnis übereinstimmen. Bei Diskrepanzen zwischen dem physischen Zufallsgerät und den Spielergebnisdaten ist das Ergebnis des physischen Zufallsgeräts als korrekt anzusehen.

: Betriebs-Audit für Gaming-Verfahrensweisen und -Praktiken

A.1 Einleitung

A.1.1 Allgemeines

In diesem Anhang werden Verfahrensweisen und Praktiken für den Spielbetrieb erläutert, die in einem Betriebs-Audit im Rahmen einer Beurteilung des interaktiven Spielsystems geprüft werden. Dies beinhaltet beispielsweise das Definieren von Spielregeln, Verwalten von Spielen, Überwachen von Spielen und Ergebnissen des Zufallszahlengenerators (RNG), Abwickeln verschiedener Spiel- und Finanz-Transaktionen, Erstellen und Verwalten progressiver Jackpots und stufenweiser Jackpots, Spielerkontenverwaltung, grundlegende, für die Risikobegrenzung relevante Praktiken sowie jegliche andere Zielsetzungen, die von der Regulierungsbehörde definiert wurden.

HINWEIS: Es wird ebenfalls anerkannt, dass zusätzliche Verfahrensweisen und Praktiken, die nicht speziell in diese Norm eingeschlossen sind, für ein Betriebs-Audit relevant und erforderlich sind, wenn dies vom Betreiber und/oder der Regulierungsbehörde innerhalb ihrer Regeln, Vorschriften und internen Mindestkontrollstandards (MICS) bestimmt wurde.

A.2 Interne Kontrollverfahren

A.2.1 Interne Kontrollverfahren

Der Betreiber muss interne Kontrollverfahren für den Spielbetrieb einrichten, aufrechterhalten, implementieren und beachten, einschließlich der Durchführung von Spiel- und Finanztransaktionen.

A.2.2 Informationsmanagement

Die internen Kontrollen des Betreibers müssen die Prozesse für die Speicherung der aufgezeichneten Informationen beinhalten, die im Abschnitt „Zu sichernde Informationen“ für einen Zeitraum von fünf Jahren oder entsprechend anderslautenden Vorgaben der Regulierungsbehörde angegeben sind.

A.2.3 Risikomanagement

Die internen Kontrollen des Betreibers müssen Details zu seinem Rahmenwerk für das Risikomanagement beinhalten, wie beispielsweise:

- a) automatische und manuelle Risikomanagement-Verfahren;
- b) Personalmanagement, einschließlich Zugangskontrollen und Aufgabentrennung;
- c) Informationen in Bezug auf Erkennung und Meldung von Betrug und verdächtigem Verhalten;
- d) Kontrollen zur Sicherstellung der regulatorischen Compliance;
- e) Beschreibung von Compliance-Standards zur Geldwäschebekämpfung, einschließlich Verfahrensweisen zur Erkennung von Strukturen zur Vermeidung von Berichtsanforderungen;
- f) Beschreibung aller Software-Anwendungen, aus denen das interaktive Spielsystem besteht;

- g) Beschreibung aller verfügbaren Spieltypen, die vom Betreiber angeboten werden können;
- h) Beschreibung der Methode zur Verhinderung von Absprachen bei Peer-to-Peer-Spielen;
- i) Beschreibung aller integrierten Drittanbieter für Services; und
- j) alle sonstigen von der Regulierungsbehörde geforderten Informationen.

A.2.4 Gesperrte Spieler

Die internen Kontrollen des Betreibers müssen die Methode zur Verhinderung der Spielteilnahme von Menschen beschreiben, die als Mitarbeitende, Subunternehmer, Direktoren, Inhaber und leitende Angestellte eines Betreibers oder als in deren Haushalt lebende Person erkannt wurden, wie von der Regulierungsbehörde gefordert.

A.2.5 Testkonten

Der Betreiber kann Testkonten einrichten, um die zahlreichen Komponenten und Prozesse eines interaktiven Spielsystems in Übereinstimmung mit internen Kontrollen des Betreibers zu testen. Hierzu gehören die folgenden Verfahrensweisen:

- a) die Verfahrensweisen zur Autorisierung von Testaktivitäten und zur Freigabe jedes Testkontos für die jeweilige Nutzung;
- b) die Verfahrensweisen für die Ausgabe von Geldmitteln zu Testzwecken, einschließlich der Bestimmung, wer befugt ist, die Geldmittel auszugeben, und des Höchstbetrags, der ausgegeben werden kann;
- c) das Pflegen von Aufzeichnungen für alle Testkonten mit Angaben zum Aktivitätszeitpunkt und Angaben zur Person, an die es herausgegeben wurde; und
- d) die Verfahrensweisen für die Überprüfung der Testaktivität, um die Rechenschaftspflicht für die zu Testzwecken genutzten Geldmittel sowie ordnungsgemäße Anpassungen von Berichten und Aufzeichnungen sicherzustellen.

A.3 Spielerkonto-Kontrollen

A.3.1 Registrierung und Verifizierung

Wenn die Registrierung von Spielerkonten manuell durch den Betreiber erfolgt, müssen Verfahrensweisen zur Erfüllung der Anforderungen für „Registrierung und Verifizierung“ implementiert werden, wie in diesem Dokument angegeben.

A.3.2 Betrügerische Konten

Der Betreiber muss über eine dokumentierte öffentliche Richtlinie für den Umgang mit Spielerkonten verfügen, bei denen eine betrügerische Nutzung erkannt wurde, wie beispielsweise:

- a) Die Speicherung von Informationen über jegliche Aktivitäten des Kontos wie erkannte betrügerische Aktivitäten, wenn der Betreiber über die erforderlichen Informationen verfügt, um geeignete Maßnahmen zu ergreifen;
- b) die vorübergehende Sperrung aller Konten, für die eine Beteiligung an betrügerischen

Aktivitäten erkannt wurde, wie die Weitergabe des Zugangs an minderjährige Personen durch einen Spieler; und

- c) die Handhabung von Einzahlungen und Gewinnen in Verbindung mit einem betrügerischen Konto.

A.3.3 Geschäftsbedingungen

Dem Spielteilnehmer müssen die Geschäftsbedingungen zur Verfügung gestellt werden. Während des Registrierungsverfahrens und bei einer wesentlichen Aktualisierung der Geschäftsbedingungen (d. h. über grammatikalische oder andere geringfügige Änderungen hinaus) muss der Spielteilnehmer den Geschäftsbedingungen zustimmen. Die Geschäftsbedingungen müssen:

- a) darauf hinweisen, dass nur Personen, an Spielen teilnehmen können, denen dies durch ihre Jurisdiktion gestattet ist;
- b) dem Spieler empfehlen, seine Authentifizierungsdaten (z. B. Passwort und Benutzername) sicher aufzubewahren;
- c) alle Prozesse für den Umgang mit verlorenen Authentifizierungsdaten, erzwungenen Passwortänderungen, Passwortstärken sowie anderen Elementen offenlegen, wie von der Regulierungsbehörde vorgeschrieben;
- d) Bedingungen festlegen, unter denen ein Konto für inaktiv erklärt wird, und erläutern, welche Maßnahmen in Bezug auf das Konto ergriffen werden, sobald diese Erklärung erfolgt ist;
- e) klar festlegen, was mit den Wetteinsätzen eines Spielteilnehmers geschieht, die in unterbrochenen und noch nicht entschiedenen Spielen eingesetzt wurden, bevor ein selbst auferlegter oder vom Betreiber auferlegter Ausschluss erfolgt ist, einschließlich der Rückgabe aller Wetteinsätze bzw. der Abrechnung aller Wetteinsätze, je nach Fall;
- f) Informationen über Fristen und Grenzen für Einzahlungen auf und/oder Auszahlungen von dem Konto des Spielteilnehmers enthalten, einschließlich einer klaren und präzisen Erläuterung aller Gebühren (falls zutreffend);
- g) angeben, dass der Betreiber das Recht hat:
 - i. die Einrichtung eines Kontos des Spielteilnehmers zu verweigern, wenn hierfür ein guter und ausreichender Grund vorliegt;
 - ii. Einzahlungen auf und/oder Auszahlungen von Konten von Spielteilnehmern zu verweigern, wenn hierfür ein guter und ausreichender Grund vorliegt; und
 - iii. sofern keine Ermittlungen oder Streitigkeiten im Zusammenhang mit Spielteilnehmenden ausstehen, ein Konto eines Spielteilnehmers jederzeit gemäß den Bestimmungen und Bedingungen zwischen dem Betreiber und dem Spielteilnehmer auszusetzen oder zu schließen.

A.3.4 Datenschutzrichtlinie

Dem Spielteilnehmer muss eine Datenschutzrichtlinie zur Verfügung gestellt werden. Während des Registrierungsverfahrens und bei einer wesentlichen Aktualisierung der Datenschutzrichtlinie (d. h. abgesehen von grammatikalischen oder anderen geringfügigen Änderungen) muss der Spielteilnehmer der Datenschutzrichtlinie zustimmen. In der Datenschutzrichtlinie ist anzugeben:

- a) die zu erfassenden personenbezogenen Daten;

- b) Zweck und Rechtsgrundlage für die Erhebung personenbezogener Daten und für jede Verarbeitungstätigkeit, für die eine Einwilligung eingeholt wird, einschließlich, falls von der Regulierungsbehörde gefordert, des „berechtigten Interesses“ des Betreibers (oder des/der Drittdienstleister(s)), wenn dies die gewählte Rechtsgrundlage ist (d. h. Angabe des betreffenden Interesses);
- c) Der Zeitraum, in dem die personenbezogenen Daten gespeichert werden, oder, falls kein Zeitraum festgelegt werden kann, die Kriterien, nach denen dies festgelegt wurde. Es reicht nicht aus, wenn der Betreiber angibt, dass die personenbezogenen Daten so lange gespeichert werden, wie es für die rechtmäßigen Zwecke der Verarbeitung erforderlich ist;
- d) die Bedingungen, unter denen personenbezogene Daten offengelegt werden können;
- e) eine Bestätigung, dass Maßnahmen ergriffen werden, um die unbefugte oder unnötige Offenlegung von personenbezogenen Daten zu verhindern;
- f) Identität und Kontaktdaten des Betreibers, der die Zustimmung einholt, einschließlich aller Drittanbieter, die auf diese personenbezogenen Daten zugreifen oder sie verwenden können;
- g) falls von der Regulierungsbehörde gefordert, dass der Spielteilnehmer ein Recht hat:
 - i. auf seine/ihre personenbezogenen Daten zugreifen, sie zu exportieren oder zu übertragen;
 - ii. seine/ihre personenbezogenen Daten zu berichtigen, zu löschen oder den Zugriff darauf einzuschränken;
 - iii. Einspruch gegen die Verarbeitung seiner/ihrer personenbezogenen Daten einzulegen;
 - iv. die Einwilligung zu widerrufen, wenn die Verarbeitung auf einer Einwilligung beruht;
- h) die Rechte und Möglichkeiten eines Spielteilnehmers, eine Beschwerde bei der Regulierungsbehörde einzureichen;
- i) für personenbezogenen Daten, die direkt vom Spielteilnehmer erhoben werden, ob eine gesetzliche oder vertragliche Verpflichtung zur Bereitstellung der personenbezogenen Daten besteht und welche Folgen die Nichtbereitstellung dieser personenbezogenen Daten hat;
- j) falls zutreffend und von der Regulierungsbehörde verlangt, Informationen über die Verwendung automatisierter Entscheidungsfindung seitens des Betreibers, einschließlich Profiling, und zwar zumindest in diesen Fällen, ohne dass dadurch die Einhaltung anderer rechtlicher Verpflichtungen behindert wird:
 - i. ausreichender Einblick in die Logik der automatisierten Entscheidungsfindung;
 - ii. die Bedeutung und die voraussichtlichen Folgen einer solchen Verarbeitung für den Spielteilnehmer; und
 - iii. Sicherheitsvorkehrungen im Zusammenhang mit der ausschließlich automatisierten Entscheidungsfindung, einschließlich Informationen für den Spielteilnehmer darüber, wie er die Entscheidung anfechten und eine direkte menschliche Überprüfung oder Intervention verlangen kann.

A.3.5 Sicherheit personenbezogener Daten

Alle im Zusammenhang mit dem Spielerkonto eingeholten Informationen, einschließlich personenbezogener Daten und Authentifizierungsdaten, sind im Einklang mit der Datenschutzrichtlinie und den von der Regulierungsbehörde eingehaltenen lokalen Datenschutzvorschriften und -standards zu behandeln. Sowohl personenbezogene Daten als auch Guthaben von Spielteilnehmern sind für die Zwecke der Risikobewertung als kritische Vermögenswerte zu betrachten.

- a) Alle personenbezogenen Daten, die nicht gemäß der Datenschutzrichtlinie offengelegt werden müssen, sind vertraulich zu behandeln, es sei denn, die Freigabe dieser Informationen ist gesetzlich vorgeschrieben. Dazu gehören unter anderem:
 - i. Die Höhe des Geldbetrages, der einem bestimmten Spielerkonto gutgeschrieben oder von diesem ausbezahlt wurde oder sich auf diesem befindet;
 - ii. der von einem bestimmten Spielteilnehmer in einem Spiel eingesetzte Geldbetrag;
 - iii. die Kontonummer und die Authentifizierungsdaten, die den Spielteilnehmer identifizieren; und
 - iv. Name, Adresse und andere Informationen im Besitz des Betreibers, die den Spielteilnehmer gegenüber anderen Personen als der Regulierungsbehörde oder dem Betreiber identifizieren würden.
- b) Es müssen Verfahren für die Sicherheit und den Austausch von personenbezogenen Daten, Guthaben auf Spielerkonten und anderen sensiblen Informationen vorhanden sein, die den Vorgaben der Regulierungsbehörde entsprechen, einschließlich, aber nicht beschränkt auf:
 - i. die Benennung und Identifizierung eines oder mehrerer Mitarbeiter, die die Hauptverantwortung für die Gestaltung, Umsetzung und laufende Bewertung solcher Verfahren und Praktiken tragen;
 - ii. Verfahren zur Bestimmung der Art und des Umfangs aller erfassten Informationen, der Standorte, an denen diese Informationen gespeichert werden, und der Speichermedien, auf denen diese Informationen zum Zwecke der Speicherung oder Übertragung aufgezeichnet werden können;
 - iii. die Maßnahmen, die zum Schutz der Informationen vor unbefugtem Zugriff ergriffen werden; und
 - iv. die Verfahren, die anzuwenden sind, wenn der Betreiber eine Verletzung der Datensicherheit feststellt, einschließlich der erforderlichen Benachrichtigung der Regulierungsbehörde.
- c) Falls von der Regulierungsbehörde gefordert, müssen die Spielteilnehmer die Möglichkeit haben, einen Antrag zu stellen auf:
 - i. Bestätigung, dass ihre personenbezogenen Daten verarbeitet werden;
 - ii. Zugang zu einer Kopie ihrer personenbezogenen Daten sowie zu allen weiteren Informationen über die Verarbeitung personenbezogener Daten;
 - iii. Aktualisierung ihrer personenbezogenen Daten; und
 - iv. Löschung ihrer personenbezogenen Daten und/oder Einschränkung der Verarbeitung personenbezogener Daten.
- d) Es müssen Verfahren vorhanden sein, um entsprechende Anträge von Spielteilnehmern zu erfassen und zu bearbeiten, einschließlich der Führung von Aufzeichnungen über solche Anträge und der Angabe von Gründen für den Spielteilnehmer, wenn solche Anträge abgelehnt oder zurückgewiesen werden. Der Spielteilnehmer erhält eine Begründung, wenn der Betreiber nicht beabsichtigt, dem Ersuchen nachzukommen, sowie die notwendigen Informationen über die Möglichkeit, eine Beschwerde bei der Regulierungsbehörde einzureichen.
- e) Auf Verlangen der Regulierungsbehörde und auf Wunsch des Spielteilnehmers leitet der Betreiber die personenbezogenen Daten, die er von ein und demselben Spielteilnehmer erhalten hat, in einem strukturierten, allgemein gebräuchlichen und maschinenlesbaren Format an die Spielteilnehmer weiter und übermittelt diese Daten an einen anderen Betreiber, sofern dies technisch machbar ist. Dies gilt nur für:

- i. personenbezogene Daten, die der Spielteilnehmer dem Betreiber zur Verfügung gestellt hat, oder personenbezogene Daten, die automatisiert verarbeitet werden (d. h. dies würde jegliche Aufzeichnungen in Papierform ausschließen); und
 - ii. Fälle, in denen die Zustimmung des Spielteilnehmers die Grundlage für die Verarbeitung der personenbezogenen Daten ist oder die Daten zur Erfüllung eines Vertrags oder zur Vorbereitung eines Vertrags verarbeitet werden.
- f) Sofern von der Regulierungsbehörde gefordert, hat der Spielteilnehmer das Recht, der Verarbeitung von personenbezogenen Daten zu widersprechen:
- i. auf der Grundlage von berechtigten Interessen oder der Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt;
 - ii. im Falle einer Verwendung im Rahmen von Direktmarketing, einschließlich Profiling, soweit es mit solchen Marketingaktivitäten zusammenhängt; und
 - iii. zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken.
- g) Der Betreiber muss über Verfahren verfügen, mit denen er Anträgen von Spielteilnehmern auf Löschung personenbezogener Daten und/oder auf Verhinderung oder Einschränkung der Verarbeitung personenbezogener Daten nachkommen kann, unter anderem in folgenden Fällen:
- i. wenn die personenbezogenen Daten in Bezug auf den Zweck, für den sie ursprünglich erhoben/verarbeitet wurden, nicht mehr erforderlich sind;
 - ii. wenn der Spielteilnehmer seine Zustimmung zurückzieht;
 - iii. wenn der Spielteilnehmer der Verarbeitung der personenbezogenen Daten widerspricht und kein überwiegendes berechtigtes Interesse an der Fortsetzung der Verarbeitung besteht;
 - iv. die personenbezogenen Daten unrechtmäßig verarbeitet wurden; oder
 - v. die personenbezogenen Daten gelöscht werden müssen, um einer rechtlichen Verpflichtung nachzukommen.
- h) Sofern dies von der Regulierungsbehörde untersagt ist, darf der Betreiber keine ausschließlich automatisierte Entscheidungsfindung verwenden, wenn diese:
- i. rechtliche Auswirkungen auf den Spielteilnehmer hat, die beispielsweise dazu führen, dass der Spielteilnehmer von einer zuständigen Behörde überwacht wird; oder
 - ii. den Spielteilnehmer in ähnlicher Weise erheblich beeinträchtigt (z. B. wenn das Potenzial besteht, dass die Umstände, das Verhalten oder die Entscheidungen des Spielteilnehmers beeinflusst werden könnten).

A.3.6 Verwaltung von Guthaben der Spielteilnehmer

Es müssen Verfahren vorhanden sein, die sicherstellen, dass alle Finanztransaktionen in Übereinstimmung mit den örtlichen Handelsvorschriften und den von der Regulierungsbehörde vorgeschriebenen Anforderungen durchgeführt werden.

- a) Für den Fall, dass Finanztransaktionen nicht automatisch durch das interaktive Spielsystem durchgeführt werden können, müssen Verfahren vorhanden sein, die die Anforderungen für „Finanztransaktionen“, wie in diesem Dokument angegeben, erfüllen.
- b) Wenn Finanztransaktionen mittels elektronischer Überweisungen zugelassen sind, muss der Betreiber über entsprechende Sicherheitsmaßnahmen und Kontrollen verfügen, um Betrug im Zusammenhang mit elektronischen Überweisungen zu verhindern. Ein fehlgeschlagener Versuch einer elektronischen Überweisung kann nicht als betrügerisch angesehen werden, wenn der Spieler bei einer früheren Gelegenheit erfolgreich eine elektronische Überweisung durchgeführt

hat und keine Rückbuchungen ausstehen. Andernfalls muss der Betreiber alle folgenden Maßnahmen ergreifen:

- i. Vorübergehende Sperrung des Spielerkontos zur Untersuchung eines möglichen Betrugs nach fünf aufeinanderfolgenden fehlgeschlagenen Versuchen einer elektronischen Überweisung innerhalb eines Zeitraums von zehn Minuten oder eines von der Regulierungsbehörde festzulegenden Zeitraums. Liegen keine Beweise für einen Betrug vor, kann die Sperrung aufgehoben werden; und
 - ii. das Spielerkonto nach fünf weiteren fehlgeschlagenen Versuchen einer elektronischen Überweisung innerhalb eines Zeitraums von zehn Minuten oder eines von der Regulierungsbehörde festzulegenden Zeitraums gesperrt werden.
- c) Eine positive Identifizierung oder Authentifizierung des Spielteilnehmers muss durchgeführt werden, bevor der Spieler Geld auszahlen kann.
 - d) Der Betreiber darf nicht zulassen, dass ein Spielerkonto überzogen wird, es sei denn, dies ist auf Probleme bei der Zahlungsabwicklung zurückzuführen, die sich der Kontrolle des Betreibers entziehen.
 - e) Der Antrag eines Spielteilnehmers auf Auszahlung von Guthaben (d. h. eingezahlte und frei verfügbare Guthaben sowie gewonnene Einsätze) wird vom Betreiber innerhalb eines angemessenen Zeitraums bearbeitet, es sei denn, es liegt eine ungelöste Beschwerde/ein ungelöster Streitfall oder eine Untersuchung im Zusammenhang mit diesem Spielteilnehmer vor. Eine solche Untersuchung ist vom Betreiber zu dokumentieren und der Regulierungsbehörde zur Überprüfung vorzulegen.
 - f) Der Betreiber muss über Sicherheits- oder Genehmigungsverfahren verfügen, die gewährleisten, dass nur genehmigte Änderungen an Spielerkonten vorgenommen werden können und diese Änderungen überprüfbar sind.

A.3.7 Beschränkungen

Den Spielteilnehmern muss eine Methode zur Verfügung gestellt werden, mit der sie Beschränkungen für Spielparameter festlegen können, einschließlich, aber nicht beschränkt auf Einzahlungen und Einsätze, wie von der Regulierungsbehörde gefordert. Darüber hinaus muss der Betreiber die Möglichkeit haben, die von der Regulierungsbehörde geforderten Beschränkungen für die Spielparameter festzulegen.

- a) Sobald ein Spielteilnehmer eine Beschränkung festgelegt hat und diese vom Betreiber in Kraft gesetzt wird, darf es nur möglich sein, den Schweregrad der selbst auferlegten Beschränkungen mit einer Vorankündigung von vierundzwanzig Stunden oder auf Verlangen der Regulierungsbehörde zu verringern.
- b) Die Spielteilnehmer werden im Voraus über alle vom Betreiber auferlegten Beschränkungen und deren Gültigkeitsdatum informiert. Nach einer Aktualisierung müssen die vom Betreiber auferlegten Beschränkungen mit dem übereinstimmen, was dem Spielteilnehmer mitgeteilt wurde.
- c) Nach Erhalt einer selbst auferlegten oder vom Betreiber auferlegten Beschränkungsanweisung stellt der Betreiber sicher, dass alle angegebenen Beschränkungen sofort oder zu einem dem Spieler klar mitgeteilten Zeitpunkt (z. B. nächste Anmeldung, nächster Tag) korrekt umgesetzt werden.

A.3.8 Ausschlüsse

Die Spielteilnehmer müssen die Möglichkeit haben, sich für einen bestimmten Zeitraum oder auf unbestimmte Zeit vom Spiel auszuschließen, je nachdem, was die Regulierungsbehörde verlangt. Außerdem muss der Betreiber die Möglichkeit haben, einen Spielteilnehmer nach Maßgabe der Regulierungsbehörde vom Spiel auszuschließen.

- a) Die Spielteilnehmer erhalten eine Benachrichtigung, die den Status des Ausschlusses und allgemeine Anweisungen zur Lösung des Problems enthält, sofern dies möglich ist.
- b) Unmittelbar nach Erhalt des Ausschlusses werden keine neuen Einsätze oder Einzahlungen von diesem Spieler angenommen, bis der Ausschluss aufgehoben ist.
- c) Während des Ausschlusses wird der Spielteilnehmer nicht daran gehindert, sein Guthaben ganz oder teilweise auszuzahlen, sofern der Betreiber bestätigt, dass das Guthaben frei verfügbar ist und der Grund/die Gründe für den Ausschluss einer Auszahlung nicht entgegenstehen.
- d) Jegliche Werbe- oder Marketingmaterialien dürfen nicht an Spielteilnehmer gerichtet sein, die vom Spiel ausgeschlossen wurden.

A.3.9 Inaktive Konten

Ein Spielerkonto gilt unter den in den Allgemeinen Geschäftsbedingungen genannten Bedingungen als inaktiv. Es müssen Verfahren vorhanden sein, um:

- a) dem Spieler den Zugriff auf sein inaktives Konto erst nach einer zusätzlichen Identitätsprüfung zu gestatten;
- b) inaktive Spielerkonten, die Guthaben enthalten, vor unbefugtem Zugriff, Änderungen oder Löschung zu schützen; und
- c) nicht beanspruchte Guthaben von inaktiven Spielerkonten zu handhaben, einschließlich der Rückgabe von Restbeträgen an den Spieler, sofern möglich.

A.3.10 Kontoschließung

Die Spielteilnehmer müssen die Möglichkeit haben, ihr Spielerkonto jederzeit zu schließen, es sei denn, der Betreiber hat einen Spielteilnehmer vorübergehend vom Spiel ausgeschlossen. Ein etwaiges auf einem Konto des Spielteilnehmers vorhandenes Restguthaben wird dem Spielteilnehmer zurückerstattet, sofern der Betreiber bestätigt, dass das Guthaben frei verfügbar ist.

A.4 Allgemeine Betriebsabläufe

A.4.1 Betreiberreserven

Der Betreiber muss über Verfahren verfügen, um angemessene Barreserven zu halten und zu schützen, deren Umfang von der Regulierungsbehörde festgelegt wird, einschließlich getrennter Konten für Gelder, die für Spielerkonten gehalten werden, und Betriebsgelder, die zur Deckung aller anderen Haftungen des Betreibers verwendet werden, sofern dies von der Regulierungsbehörde vorgegeben wird.

A.4.2 Schutz von Guthaben der Spielteilnehmer

Der Betreiber muss über Verfahren verfügen, die gewährleisten, dass Gelder auf einem Betreiberkonto entweder treuhänderisch für den Spieler auf einem getrennten Konto oder auf einem Sonderkonto gehalten werden, das von einer ordnungsgemäß konstituierten juristischen Person geführt und kontrolliert wird, bei der es sich nicht um den Betreiber handelt und deren Vorstand aus einem oder mehreren Direktoren besteht, die vom Betreiber und von allen mit dem Betreiber verbundenen oder von ihm kontrollierten Unternehmen unabhängig sind. Darüber hinaus muss der Betreiber über Verfahren verfügen, die nach vernünftigem Ermessen so gestaltet sind, dass:

- a) sichergestellt wird, dass die aus dem Glücksspiel generierten Gelder gesichert und verbucht werden;
- b) deutlich gemacht wird, dass die Gelder auf dem getrennten Konto nicht dem Betreiber gehören und nicht für andere Gläubiger als den Spieler, dessen Gelder gehalten werden, verfügbar sind; und
- c) die Vermischung von Geldern auf dem getrennten Konto mit anderen Geldern, einschließlich, aber nicht beschränkt auf Gelder des Betreibers, verhindert wird.

A.4.3 Besteuerung

Der Betreiber muss über ein Verfahren verfügen, um alle steuerpflichtigen Gewinne (Einzelgewinne oder Gesamtgewinne über einen bestimmten Zeitraum) zu ermitteln und die erforderlichen Informationen gemäß den steuerlichen Anforderungen der jeweiligen Regulierungsbehörde bereitzustellen.

HINWEIS: Gewonnene Beträge, die ein von der Rechtsprechung festgelegtes Limit überschreiten, erfordern eine entsprechende Dokumentation, bevor der Betrag dem Gewinner ausgezahlt wird.

A.4.4 Beschwerde-/Streitbeilegungsverfahren

Der Betreiber muss dem Spielteilnehmer ein Verfahren zur Verfügung stellen, mit dem eine Beschwerde/Streitigkeit eingereicht und die Regulierungsbehörde benachrichtigt werden kann, wenn diese Beschwerde/Streitigkeit vom Betreiber nicht bearbeitet wurde oder nicht bearbeitet werden kann, oder unter anderen Umständen, dies in den Rechtsvorschriften der Regulierungsbehörde vorgegeben ist.

- a) Die Spielteilnehmer müssen in der Lage sein, Beschwerden/Streitigkeiten rund um die Uhr zu protokollieren.
- b) Aufzeichnungen über den gesamten Schriftverkehr im Zusammenhang mit einer Beschwerde/einem Streitfall sind für fünf Jahre oder nach Maßgabe der Regulierungsbehörde aufzubewahren.
- c) Zwischen dem Betreiber und der Regulierungsbehörde muss ein dokumentiertes Verfahren für die Meldung und Beilegung von Beschwerden/Streitigkeiten bestehen.

A.4.5 Informationen zum Schutz von Spielteilnehmern

Die Informationen zum Schutz von Spielteilnehmern müssen dem Spielteilnehmer zur Verfügung gestellt werden. Die Informationen zum Schutz von Spielteilnehmern müssen mindestens Folgendes enthalten:

- a) Informationen über potenzielle Risiken im Zusammenhang mit exzessivem Spiel und darüber, an welche Stellen man sich im Falle eines Spielproblems wenden kann;
- b) eine Erklärung, dass Minderjährigen die Teilnahme am Glücksspiel nicht gestattet ist;
- c) eine Liste der verfügbaren Maßnahmen zum Schutz von Spielteilnehmern, die vom Spielteilnehmer in Anspruch genommen werden können, wie z.B. ein selbst auferlegter Ausschluss, sowie Informationen darüber, wie diese Maßnahmen in Anspruch genommen werden können;
- d) Mechanismen, die zur Erkennung einer unbefugten Nutzung des Kontos eingesetzt werden können, wie z. B. die Überprüfung von Kontoauszügen anhand bekannter Einzahlungen;
- e) Kontaktinformationen oder andere Möglichkeiten zur Meldung einer Beschwerde/eines Streitfalls; und
- f) Kontaktinformationen für die Regulierungsbehörde und/oder ein Link zu deren Website.

HINWEIS: Alle Links zu Diensten für problematisches Glücksspiel, die von Dritten angeboten werden, sind vom Betreiber regelmäßig zu überprüfen. Interaktive Spiele dürfen nicht stattfinden, wenn die Links, die Informationen zum Spielerschutz enthalten, nicht angezeigt werden oder nicht funktionieren. Ist der Link nicht mehr oder über einen längeren Zeitraum nicht verfügbar, muss der Betreiber einen alternativen Unterstützungsdienst anbieten.

A.4.6 Verantwortungsbewusstes Spielen

Der Betreiber muss über Richtlinien und Verfahren verfügen, die den Umgang mit Spielteilnehmern erleichtert, wenn deren Spielverhalten auf das Risiko der Entwicklung eines Glücksspielproblems hindeutet. Mitarbeiter, die direkt mit den Spielteilnehmern interagieren, müssen entsprechend geschult werden, um sicherzustellen, dass sie über angemessenes Verständnis in Bezug auf problematisches Spielverhalten verfügen und wissen, wie sie in solchen Situationen zu reagieren haben.

A.4.7 Chat-Funktionen

Für Fälle, in denen der Betreiber die Nutzung von Chat-Funktionen vorsieht, die es dem Spielteilnehmer ermöglichen, direkt mit dem Betreiber und/oder anderen Spielteilnehmern zu kommunizieren, muss ein festgelegtes Verfahren bestehen, einschließlich der Aufbewahrung von Chat-Protokollen für einen Zeitraum von neunzig Tagen oder wie von der Regulierungsbehörde festgelegt. Zusätzlich muss die E-Mail-Korrespondenz zwischen dem Spielteilnehmer und dem Betreiber für den gleichen Zeitraum aufbewahrt werden.

A.5 Spielregeln und -inhalte

A.5.1 Spielregeln

Der Begriff Spielregeln bezieht sich auf alle schriftlichen, grafischen und akustischen Informationen, die der Öffentlichkeit über den Spielbetrieb zur Verfügung gestellt werden. Der Betreiber muss umfassende Spielregeln festlegen und einhalten, die von der Regulierungsbehörde genehmigt werden müssen.

- a) Die Spielregeln müssen vollständig, eindeutig und für den Spielteilnehmer nicht irreführend oder unfair sein.
- b) Mündlich (durch Ton oder Stimme) zur Verfügung gestellte Spielregeln müssen zusätzlich in schriftlicher Form angezeigt werden.
- c) Die Spielregeln müssen in einer Farbe dargestellt werden, die sich von der Hintergrundfarbe abhebt, um zu gewährleisten, dass alle Informationen deutlich sichtbar/lesbar sind.
- d) Der Betreiber führt ein Protokoll über alle Änderungen der Spielregeln in Bezug auf das Spielen.
- e) Werden die Spielregeln für die angebotenen Spiele geändert, sind alle Regeländerungen mit einem Zeit- und Datumsstempel zu versehen, aus dem hervorgeht, welche Regel im jeweiligen Zeitraum gilt. Gelten für ein Spiel mehrere Regeln, so wendet der Betreiber die Regeln an, die zum Zeitpunkt der Annahme des Wetteinsatzes galten.

A.5.2 Spielregeln Inhalt

Die folgenden Informationen werden dem Spielteilnehmer zur Verfügung gestellt. Die Funktionalität zur Anzeige der in diesem Abschnitt geforderten Informationen muss über die Spielerschnittstelle oder eine für den Spieler zugängliche Seite angezeigt werden:

- a) die Methoden zur Einzahlung auf ein Spielerkonto (z. B. Bargeld, Barscheck, Bankscheck, Überweisung, Zahlungsanweisung, Debitkarte, Kreditkarte, elektronische Überweisung usw.), einschließlich einer genauen und eindeutigen Erläuterung aller Gebühren (falls zutreffend);
- b) soweit von der Regulierungsbehörde zugelassen, alle Preise, die in Form von Waren, Renten, Pauschalzahlungen oder Zahlungsplänen anstelle von Barauszahlungen für jedes Spiel angeboten werden, das einen solchen Preis enthält;
- c) die Verfahren, anhand derer nicht behebbare Fehlfunktionen der Hardware/Software gehandhabt werden, einschließlich der Fälle, in denen ein solches Verfahren zur Annullierung von Auszahlungen oder Spielen führt;
- d) die Verfahren für den Umgang mit Unterbrechungen, die durch die Trennung des Spielteilnehmers von der Spielplattform verursacht werden, wenn das Ergebnis eines Spiels durch die Zeit, die für die Reaktion auf ein Spielereignis benötigt wird, beeinflusst wird;
- e) Informationen darüber, was mit den Einsätzen des Spielteilnehmers geschieht, die in unterbrochenen Spielen platziert wurden, welches nicht abgerechnet wurde, und wie diese gehandhabt werden, wenn sie über den festgelegten Zeitraum hinaus nicht abgerechnet werden;
- f) eine Beschreibung gesperrter Spielteilnehmer, einschließlich der für sie geltenden Teilnahmebeschränkungen;
- g) für jeden progressiven Jackpot oder stufenweisen Jackpot:
 - i. die Unzulänglichkeiten des Kommunikationsmediums für das Spiel und wie sich dies auf die Spielteilnehmer in Bezug auf den Jackpot auswirken kann;
 - ii. ein maximales Auszahlungslimit (oder eine „Obergrenze“) und/oder zeitliche Begrenzung, die durch den Jackpot unterstützt wird;
 - iii. wie der Jackpot finanziert und festgelegt wird; und

- iv. jegliche geplante oder ungeplante Aufhebung eines Jackpots, einschließlich der Frage, wie mit ausstehenden Beiträgen umgegangen wird, um die Fairness gegenüber den Spielteilnehmern zu gewährleisten.

A.5.3 Angebote für Anreizprämien

Ein Betreiber kann Anreizprämien anbieten, bei denen es sich um Gutscheine und/oder Preise handelt, die nicht in der Auszahlungstabelle eines Spiels enthalten sind und auf vorher festgelegten Ereignissen oder Kriterien basieren, die durch die Parameter des interaktiven Spielsystems festgelegt sind.

- a) Spielteilnehmer müssen in der Lage sein, in den Spielregeln auf klare und eindeutige Bestimmungen zu allen verfügbaren Angeboten für Anreizprämien zuzugreifen. Diese müssen mindestens Folgendes umfassen:
 - i. das Datum und die Uhrzeit der Veröffentlichung;
 - ii. das Datum und die Uhrzeit, zu der das Angebot in Kraft tritt und abläuft;
 - iii. Spielberechtigung, einschließlich etwaiger Teilnahmebeschränkungen;
 - iv. jegliche Einschränkungen oder Bedingungen für die Auszahlung von Geldbeträgen;
 - v. Einsatzanforderungen und -beschränkungen je nach Art des Spiels, Spielthemas und/oder der Auszahlungstabelle;
 - vi. wie der Spielteilnehmer benachrichtigt wird, wenn er eine Anreizprämie erhalten hat;
 - vii. die Reihenfolge, in der Guthaben für Einsätze verwendet werden; und
 - viii. Regeln für die Stornierung.
- b) Der Betreiber stellt eine klare und deutliche Methode zur Verfügung, mit der ein Spieler seine Teilnahme an einem Anreizprämienangebot, bei dem eingeschränkte Anreizgutscheine verwendet werden, beenden kann.
 - i. Auf Anfrage teilt der Betreiber dem Spieler mit, welcher Betrag an unbeschränkten Spielergeldern bei einer Beendigung der Teilnahme zurückerstattet wird und welcher Wert an eingeschränkten Anreizgutscheinen vom Spielerkonto entfernt wird.
 - ii. Entscheidet sich der Spielteilnehmer für die Beendigung einer Teilnahme, so werden die auf dem Spielerkonto verbliebenen nicht zweckgebundenen Spielerguthaben gemäß den Bedingungen des Angebots zurückerstattet.
- c) Sobald ein Spielteilnehmer die Bedingungen eines Anreizprämienangebots erfüllt hat, darf der Betreiber die während der Teilnahme an dem Angebot erzielten Gewinne nicht begrenzen (d. h. die eingeschränkten Anreizgutscheine des Angebots werden zu uneingeschränkten Anreizgutscheinen).

A.5.4 Wettbewerbe/Turniere

Ein Wettbewerb/Turnier, bei dem ein Spielteilnehmer die Möglichkeit hat, die Teilnahme an einem wettbewerbsorientierten Spiel gegen andere Spielteilnehmer entweder zu erwerben oder zu erhalten, ist zulässig, sofern die folgenden Regeln eingehalten werden:

- a) Die Regeln werden den Spielteilnehmern in den Spielregeln vor der Anmeldung zum Wettbewerb/Turnier zur Einsichtnahme zur Verfügung gestellt. Die Regeln müssen mindestens Folgendes umfassen:

- i. alle Bedingungen, die registrierte Spielteilnehmer erfüllen müssen, um sich für die Teilnahme und das Weiterkommen im Wettbewerb/Turnier zu qualifizieren;
 - ii. spezifische Informationen zu jedem einzelnen Wettbewerb/Turnier, einschließlich der verfügbaren Preise oder Prämien und der Verteilung der Gelder auf der Grundlage bestimmter Ergebnisse; und
 - iii. den Namen der Organisation (oder der Personen), die den Wettbewerb/das Turnier im Namen des Betreibers oder in Verbindung mit diesem durchgeführt haben, falls zutreffend.
- b) Es müssen Verfahren vorhanden sein, um die Ergebnisse jedes Wettbewerbs/Turniers zu erfassen und den registrierten Spielteilnehmern innerhalb eines angemessenen Zeitraums öffentlich zugänglich zu machen. Die Ergebnisse eines jeden Wettbewerbs/Turniers werden nach ihrer Veröffentlichung auf Anfrage zur Verfügung gestellt. Die Ergebnisse müssen Folgendes umfassen:
- i. Name des Wettbewerbs/Turniers;
 - ii. Datum/Zeit des Wettbewerbs/Turniers;
 - iii. Gesamtzahl der Teilnehmer;
 - iv. Höhe der Teilnahmegebühren;
 - v. Gesamtpreispool; und
 - vi. für jede Gewinnerkategorie gezahlter Betrag.

HINWEIS: Bei kostenlosen Wettbewerben/Turnieren (d.h. ein registrierter Spielteilnehmer zahlt keine Teilnahmegebühr) werden die oben genannten Informationen aufgezeichnet, mit Ausnahme der Anzahl der Teilnehmer, der Höhe der Teilnahmegebühren und des Gesamtpreispools.

A.6 Verfahren und Kontrollen für Glücksspiele

A.6.1 Bewertung der theoretischen und tatsächlichen Auszahlungsquote für den Spielteilnehmer

Der Betreiber muss genaue und aktuelle Unterlagen (z. B. PAR Sheets) führen, aus denen die theoretischen Auszahlungsquoten (Return to Player oder RTP) für jedes Hausbank-Spiel auf der Grundlage angemessener Einsätze sowie die Anzahl der spielbaren Guthaben, der Auszahlungsplan und andere Informationen für die jeweilige Spielart hervorgehen. Darüber hinaus:

- a) Für jedes Spiel sind Aufzeichnungen zu führen, aus denen der ursprüngliche Prozentsatz der theoretischen Auszahlungsquote, die Daten und die Art der Änderungen, die den Prozentsatz der theoretischen Auszahlungsquote des Spiels beeinflussen, sowie die Neuberechnung des Prozentsatzes der theoretischen Auszahlungsquote aufgrund der Änderungen hervorgehen.
- b) Jede Änderung des Prozentsatzes der theoretischen Auszahlungsquote eines Spiels, einschließlich der Hinzufügung und/oder Änderung des progressiven Jackpots oder der stufenweisen Erhöhung des Jackpots, hat zur Folge, dass dieses Spiel für alle Berichte und Aufzeichnungen als neu behandelt wird.
- c) Werden Anreizprämien in die Berichte und Aufzeichnungen für das Spiel aufgenommen, so muss dies in einer Weise geschehen, die eine Verzerrung der tatsächlichen Prozentsätze der theoretischen Auszahlungsquote der betroffenen Auszahlungstabelle verhindert.

- d) Der Betreiber muss über Verfahren verfügen, mit denen er den Prozentsatz der theoretischen und tatsächlichen Auszahlungsquote regelmäßig vergleicht, um große Abweichungen zwischen diesen beiden Werten festzustellen, zu untersuchen und zu beheben.

A.6.2 Überwachung des Spiels und der Ausgabe des Zufallsgenerators

Der Betreiber muss über Verfahren zur Überwachung des Spiels und der Ausgabe des Zufallsgenerators in einem bestimmten, von der Regulierungsbehörde vorgeschriebenen Turnus oder Umfang verfügen. Zweck der Überwachung ist die frühzeitige Erkennung von abnormalem Verhalten, um rechtzeitig geeignete Abhilfemaßnahmen zu ermöglichen. Jegliche Auffälligkeiten (z. B. der Prozentsatz der tatsächlichen Auszahlungsquote für den Zeitraum liegt außerhalb des erwarteten Bereichs) führen dazu, dass ein Fehler protokolliert und zur Untersuchung eskaliert wird. Die Überwachung der bewährten Verfahren umfasst eine unabhängige Zuordnung zwischen Ausgabe des Zufallsgenerators und Spielsymbolen, um die Verwendung von Spielsymbolen zu überprüfen. Die Protokolle der Ausgabe des Zufallsgenerators und der Spielsymbole können als Überwachungsmaßnahme geführt und überprüft werden.

A.6.3 Deaktivierung von Spielen

Es müssen festgelegte Verfahren für die Deaktivierung eines Spiels oder einer Spielaktivität vorhanden sein. Wenn ein Spiel oder eine Spielaktivität deaktiviert wird, ist ein Eintrag in ein Prüfprotokoll zu erfolgen, der das Datum und die Uhrzeit der Deaktivierung und den entsprechenden Grund enthält.

A.6.4 Vorgehensweise bei Spielunterbrechungen

Es müssen festgelegte Verfahren für die Vorgehensweise bei Spielunterbrechungen vorhanden sein. Wenn ein Spiel aufgrund einer Aktion des interaktiven Spielsystems nicht fortgesetzt werden kann, muss der Betreiber:

- a) Aller Einsätze an den/die Spielteilnehmer des Spiels zurückzahlen;
- b) die Guthabenanzeige(n) oder den/die Kontostand/Kontostände der Spielteilnehmer sowie den Spielverlauf aktualisieren;
- c) die Regulierungsbehörde über die Umstände des Vorfalls informieren; und
- d) das Spiel deaktivieren, wenn es wahrscheinlich ist, dass das Spiel von demselben Fehler betroffen ist.

A.6.5 Verfahren für progressive und stufenweise Jackpots

Der Betreiber muss interne Kontrollverfahren für den Jackpot-Betrieb einrichten, aufrechterhalten, umsetzen und einhalten, einschließlich der folgenden:

- a) Wenn Jackpot-Beiträge Teil der Berechnungen der Auszahlungsquote sind, ist sicherzustellen, dass die Beiträge nicht mit den Einnahmen gleichgesetzt werden.
- b) Anpassungen und Übertragungen von Jackpots, falls unterstützt.

- c) Für große Jackpot-Auszahlungen, die einen bestimmten, von der Regulierungsbehörde festgelegten Wert überschreiten:
 - i. Verfahren zur Überprüfung des Jackpots und zur Auszahlung, einschließlich unabhängiger Abstimmung und Freigabe durch den Betreiber;
 - ii. Auszahlung, wenn mehrere Jackpot-Auslöser auftreten und keine definitive Möglichkeit besteht, festzustellen, welcher Auslöser zuerst eingetreten ist (es sei denn, dies wird automatisch vom interaktiven Spielsystem gehandhabt); und
 - iii. Auszahlungsoptionen für Jackpot-Gewinne, einschließlich Informationen für regelmäßige Zahlungen.
- d) Bei Jackpots mit Parametern, die nach der Ersteinrichtung konfigurierbar sind, Durchführung eines unabhängigen Abgleichs von Jackpot-Beiträgen und -Auszahlungen, um sicherzustellen, dass alle abgezogenen Jackpot-Erhöhungen:
 - i. an die Spielteilnehmer als Jackpot-Auszahlungen ausgezahlt wurden;
 - ii. als Teil von Jackpot-Auszahlungen angezeigt werden; oder
 - iii. auf separaten Konten gehalten werden, die nachweislich als Teil zukünftiger Jackpot-Auszahlungen an die Spielteilnehmer ausgezahlt werden.
- e) Verfahren zur Stilllegung von Jackpots, einschließlich Verfahren zur Verteilung von Beiträgen an einen anderen Jackpot.

A.7 Verfahren und Kontrollen für „Peer-to-Peer (P2P)“-Spielsitzungen

A.7.1 Shills und Proposition-Spieler

Der Betreiber muss über Verfahren verfügen, die sicherstellen, dass der Spielteilnehmer nicht durch Spielteilnehmer benachteiligt wird, die mit Hausgeld (Shills) spielen oder durch Spieler, die an einer P2P-Spielsitzung teilnehmen. Es müssen die folgenden Risiken gemildert werden:

- a) Die Shills und Proposition-Spieler müssen für alle anderen Spielteilnehmer dieser P2P-Spielsitzung klar erkennbar sein;
- b) die Kontrollen des Betreibers müssen den Konflikt zwischen der Rolle des Shill- oder Proposition-Spielers und der Rolle des Spielbegleiters, der Zugang zur Betriebsumgebung (sowohl physisch als auch virtuell) hat, und Spiele manipulieren kann oder über Informationen verfügt, die allen anderen Spielteilnehmern nicht zur Verfügung stehen, um daraus einen Vorteil zu ziehen, entschärfen;
- c) der Betreiber darf keinen Gewinn (über den Rake hinaus) aus dem Spiel ziehen;
- d) wenn der Einsatz des Shill- oder Proposition-Spielers vom Betreiber finanziert wird, dürfen weder der Betreiber noch der Shill- oder Proposition-Spieler von dem Spiel profitieren, die Gelder dürfen nicht ausgezahlt werden und gelten somit letztendlich als verloren/gespielt; und
- e) es müssen Verfahren vorhanden sein, um dem Risiko zu begegnen, dass der Shill- oder Proposition-Spieler motiviert ist, persönliche Einsätze über den Auftrag des stimulierenden Spiels hinaus zu schützen. Wenn der Shill- oder Proposition-Spieler private Einsätze riskiert, darf der Shill- oder Proposition-Spieler keine Kenntnis von Software oder anderen personenbezogenen Daten haben (der Shill- oder Proposition-Spieler ist ein unabhängiger Auftragnehmer ohne vorherige Beziehung zum Betreiber).

A.7.2 Verfolgung von P2P-Spielsitzungen

Der Betreiber muss über ein Verfahren verfügen, um alle P2P-Spielsitzungen jedes Spielteilnehmers zu verfolgen, einschließlich der Nachverfolgung:

- a) die für jedes Spiel aufgezeichneten „Spielinformationen“, einschließlich der gegnerischen Spielteilnehmer; und
- b) die Wahl des Spielteilnehmers für die P2P-Spielsitzung sowie die Fälle, in denen der Spielteilnehmer wiederholt P2P-Spielsitzungen betritt und verlässt, ohne zu spielen, bis er seine bevorzugte P2P-Spielsitzung erreicht.

A.7.3 Meldung verdächtiger Spielteilnehmer

Der Betreiber stellt eine Methode zur Verfügung, mit der ein Spielteilnehmer einen Verdacht auf Betrug, geheime Absprachen oder die Verwendung von Bots oder anderer nicht autorisierter Spielersoftware durch andere Spielteilnehmer melden kann, um sich einen unfairen Vorteil während der P2P-Spielsitzung zu verschaffen.

A.8 Kontrollverfahren

A.8.1 Überwachung auf geheime Absprachen und Betrug

Der Betreiber ergreift Maßnahmen zur Verringerung des Risikos von geheimen Absprachen oder Betrug, einschließlich Verfahren für:

- a) Identifizierung und/oder Verweigerung verdächtiger Wetteinsätze, die auf Betrug, Manipulation, Beeinträchtigung des regulären Spielablaufs oder Verstöße gegen die Integrität eines Spiels, auf das gesetzt wurde, hinweisen könnten.
- b) Angemessenes Erkennen von unregelmäßigen Mustern oder Serien von Einsätzen, um geheime Absprachen zwischen Spielern in P2P-Spielsitzungen zu verhindern, einschließlich der folgenden Arten von Absprachen:
 - i. Chip Dumping – eine Absprache, bei der sich zwei oder mehr Spieler gegenseitig helfen, im Spiel zu bleiben, d. h. Spielteilnehmer verlieren bei einer Hand mit einer sicheren Gewinnkombination absichtlich, um auf diese Weise einem anderen Spieler Chips zu überlassen;
 - ii. Soft-Play – eine Absprachemethode, bei der ein oder mehrere Spielteilnehmer darauf verzichten, gegen einen anderen Spielteilnehmer zu spielen, wenn ein solches Verhalten nach den normalen Spielpraktiken unangemessen ist (z. B. wenn ein Spielteilnehmer das Spiel verlässt, obwohl der Sieg sicher ist);
 - iii. Best-Hand-Spiel – eine Absprache zwischen zwei oder mehr Spielern, dass immer nur derjenige spielt, der das beste Ergebnis hat, während der andere oder die anderen das Spiel verlassen; und
 - iv. Chat Collusion – eine Absprache wird durch den Austausch relevanter Informationen in Bezug auf das aktuelle Spiel oder eine Reihe von Spielen erreicht.

- c) Angemessenes Erkennen und Verhindern von Situationen, in denen Spieler in Spielen Bots oder andere nicht autorisierte Spieler-Software verwenden, um sich einen unfairen Vorteil während des Spiels zu verschaffen, wie z. B.:
 - i. Vorhersage des Ergebnisses eines Spiels;
 - ii. bei Kartenspielen Verfolgung der gespielten Karten und der noch zu spielenden Karten;
 - iii. Analyse der Wahrscheinlichkeit des Auftretens eines Ereignisses im Zusammenhang mit einem Spiel; oder
 - iv. Analyse der Spiel- oder Einsatzstrategie, die in einem Spiel verwendet werden soll, es sei denn, dies ist nach den Spielregeln zulässig.

A.8.2 Überwachung zum Zweck der Geldwäschebekämpfung

Der Betreiber ist verpflichtet, Verfahren und Richtlinien zur Geldwäschebekämpfung zu entwickeln und umzusetzen, die den Risiken des interaktiven Glücksspiels in Bezug auf Geldwäsche und Terrorismusfinanzierung angemessen Rechnung tragen. Die Verfahren und Richtlinien zur Geldwäschebekämpfung müssen mindestens Folgendes vorsehen:

- a) ein System interner Kontrollen, um die ständige Einhaltung der lokalen Bestimmungen und Vorgaben zur Geldwäschebekämpfung der Regulierungsbehörde zu gewährleisten;
- b) aktuelle Schulungen der Mitarbeiter zur Erkennung ungewöhnlicher oder verdächtiger Transaktionen;
- c) Zuweisung einer oder mehrerer Personen, die für alle Bereiche der Geldwäschebekämpfung durch den Betreiber verantwortlich sind, einschließlich der Meldung ungewöhnlicher oder verdächtiger Transaktionen;
- d) Überwachung der Eröffnung und Schließung von Spielerkonten in kurzen Zeiträumen sowie von Ein- und Auszahlungen, ohne dass es mit diesem Guthaben zu einem Spiel kommt;
- e) Gewährleistung, dass aggregierte Transaktionen über einen definierten Zeitraum möglicherweise weitere Sorgfaltsprüfungen erfordern und der/den zuständigen Organisation(en) gemeldet werden können, wenn sie den von der Regulierungsbehörde vorgeschriebenen Schwellenwert überschreitet;
- f) Einsatz automatischer Datenverarbeitungssysteme zur Unterstützung der Einhaltung der Vorschriften; und
- g) regelmäßige unabhängige Tests zur Überprüfung der Einhaltung der Vorschriften in dem von der Regulierungsbehörde vorgeschriebenen Umfang und mit der vorgeschriebenen Häufigkeit. Über alle Tests sind Protokolle zu führen.

: Betriebs-Audit für technische Sicherheitskontrollen

B.1 Einleitung

B.1.1 Allgemeines

Dieser Anhang enthält technische Sicherheitskontrollen, die im Rahmen eines Betriebs-Audits als Teil der Bewertung des interaktiven Glücksspielsystems überprüft werden. Dies beinhaltet beispielsweise eine Prüfung der betrieblichen Prozesse, die wichtig für die Compliance sind, Penetrationstests mit Schwerpunkt auf externer und interner Infrastruktur sowie Anwendungen, die personenbezogene Daten und/oder sensible Daten übertragen, speichern und/oder verarbeiten sowie jegliche anderen von der Regulierungsbehörde definierten Zielsetzungen. Die in diesem Anhang beschriebenen Sicherheitskontrollen gelten für die folgenden kritischen Komponenten des Systems:

- a) Komponenten, die personenbezogene Daten und andere sensible Informationen aufzeichnen, speichern, verarbeiten, weitergeben, übermitteln oder abrufen (z. B. Validierungsnummern, Authentifizierungsnachweise usw.);
- b) Komponenten, die Zufallszahlen zur Bestimmung des Ergebnisses eines Spielteilnehmers erzeugen, übermitteln oder verarbeiten;
- c) Komponenten, die die Ergebnisse des aktuellen Stands des Einsatzes eines Spielteilnehmers speichern;
- d) Zugangs- und Ausgangspunkte zu den oben genannten Komponenten (andere Systeme, die direkt mit kritischen Kernsystemen kommunizieren); und
- e) Kommunikationsnetze, über die personenbezogene Daten und andere sensible Informationen übertragen werden.

HINWEIS: Es wird ebenfalls anerkannt, dass zusätzliche Verfahrensweisen und Praktiken, die nicht speziell in diese Norm eingeschlossen sind, für ein Betriebs-Audit relevant und erforderlich sind, wenn dies vom Betreiber und/oder der Regulierungsbehörde innerhalb ihrer Regeln, Vorschriften und internen Mindestkontrollstandards (MICS) bestimmt wurde.

B.2 Betrieb und Sicherheit des Systems

B.2.1 Systemabläufe

Der Betreiber ist für die Dokumentation und Einhaltung der relevanten Verfahren und Sicherheitsstandards des interaktiven Spielsystems verantwortlich, wie von der Regulierungsbehörde gefordert, einschließlich Verfahren für:

- a) Überwachung der kritischen Komponenten und der Datenübertragung des gesamten Systems, einschließlich der Kommunikation, der Datenpakete, der Netzwerke sowie der Komponenten und Datenübertragungen jeglicher Dienste Dritter, mit dem Ziel, Integrität, Zuverlässigkeit und Zugänglichkeit zu gewährleisten;

- b) Aufrechterhaltung aller Sicherheitsaspekte des Systems, um eine sichere und zuverlässige Kommunikation zu gewährleisten, einschließlich des Schutzes vor Hackerangriffen oder Manipulationen;
- c) Definition, Überwachung und Dokumentation sowie Meldung, Untersuchung, Reaktion auf und Behebung von Sicherheitsvorfällen, einschließlich festgestellter Verstöße und vermuteter oder tatsächlicher Hackerangriffe oder Manipulationen des Systems;
- d) Überwachung und Anpassung des Ressourcenverbrauchs und Führung eines Protokolls der Systemleistung, einschließlich einer Funktion zur Erstellung von Leistungsberichten;
- e) Untersuchung, Dokumentation und Behebung von Störungen, die Folgendes betreffen:
 - i. Ermittlung der Ursache der Störung;
 - ii. Überprüfung der einschlägigen Aufzeichnungen, Berichte, Protokolle und Überwachungsprotokolle;
 - iii. Reparatur oder Austausch der kritischen Komponente;
 - iv. Überprüfung der Integrität der kritischen Komponente vor ihrer Wiederinbetriebnahme;
 - v. Einreichung eines Störungsberichts bei der Regulierungsbehörde und Erfassung von Datum, Uhrzeit und Grund der Störung sowie Datum und Uhrzeit der Wiederherstellung des Systems; und
 - vi. Annullierung von Spielen und Zahlungen, wenn eine vollständige Wiederherstellung nicht möglich ist.

B.2.2 Physischer Standort von Servern

Der/die Server des interaktiven Spielsystems muss/müssen an einem oder mehreren sicheren Standorten untergebracht sein, die sich lokal innerhalb eines einzigen Standortes befinden können oder nach Maßgabe der Regulierungsbehörde außerhalb des Standortes aufgestellt werden können. Darüber hinaus müssen diese sicheren Standorte:

- a) einen ausreichenden Schutz vor Veränderungen, Manipulationen oder unbefugtem Zugriff bieten;
- b) mit einem Überwachungssystem ausgestattet sein, das den von der Regulierungsbehörde eingeführten Verfahren entspricht;
- c) durch Sicherheitszonen und geeignete Zugangskontrollen geschützt sein, um sicherzustellen, dass der Zugang nur befugtem Personal vorbehalten ist;
 - i. der physische Zugang muss über ein Multifaktor-Authentifizierungsverfahren erfolgen, es sei denn, der Standort ist ständig mit Personal besetzt;
 - ii. alle Versuche des physischen Zugangs werden in einem sicheren Protokoll aufgezeichnet; und
- d) mit Kontrollen ausgestattet sein, die einen physischen Schutz vor Schäden durch Feuer, Überschwemmung und andere Formen von Naturkatastrophen oder vom Menschen verursachten Katastrophen (z. B. Wirbelstürme, Erdbeben usw.) gewährleisten.

B.2.3 Logische Zugangskontrolle

Das interaktive Spielsystem muss logisch gegen unbefugten Zugang durch von der Regulierungsbehörde zugelassene Authentifizierungsdaten wie Passwörter, Multifaktor-

Authentifizierung, digitale Zertifikate, PINs, Biometrie und andere Zugangsmethoden (z. B. Magnetstreifen, kontaktlose Chipkarten, eingebettete Chipkarten) gesichert sein.

- a) Jedes Benutzerkonto verfügt über einen eigenen individuellen Authentifizierungsnachweis, dessen Bereitstellung durch ein förmliches Verfahren kontrolliert wird, das eine regelmäßige Überprüfung der Zugangsrechte und -privilegien umfasst. Die Verwendung allgemeiner Konten ist zu begrenzen, und wenn sie verwendet werden, sind die Gründe für ihre Verwendung förmlich zu dokumentieren.
- b) Die Authentifizierungsdaten für geheime Informationen werden entweder manuell oder durch Systeme verwaltet, die Änderungen der Authentifizierung automatisch aufzeichnen und Änderungen der Authentifizierungsdaten erzwingen.
- c) Alle im System gespeicherten Authentifizierungsdaten müssen entweder verschlüsselt oder mit kryptografischen Algorithmen gehasht werden, die den aktuellen Industriestandards (z. B. ISO/IEC 19790, FIPS 140-2 oder gleichwertig) entsprechen.
- d) Ein Verfahren zum Zurücksetzen von Authentifizierungsdaten (z. B. bei vergessenen Passwörtern) muss mindestens so sicher sein wie die primäre Methode. Für diese Zwecke muss eine Multifaktor-Authentifizierung implementiert werden.
- e) Verlorene oder gefährdete Authentifizierungsdaten und Authentifizierungsdaten ausgeschiedener Nutzer sind so bald wie möglich zu deaktivieren, zu sichern oder zu vernichten.
- f) Das System muss über mehrere Sicherheitszugriffsstufen verfügen, um verschiedene Zugriffsklassen auf den Server zu kontrollieren und zu beschränken, einschließlich der Anzeige, Änderung oder Löschung kritischer Dateien und Verzeichnisse. Es müssen Verfahren vorhanden sein, um jedem Benutzer Zugriffsrechte und Privilegien zuzuweisen, diese zu überprüfen, zu ändern und zu entziehen, einschließlich:
 - i. Ermöglichen der Verwaltung von Benutzerkonten unter Gewährleistung einer angemessenen Aufgabentrennung.
 - ii. Begrenzung der Benutzer, die über die erforderlichen Berechtigungen zur Anpassung kritischer Systemparameter verfügen.
 - iii. Durchsetzung angemessener Parameter für die Authentifizierungsdaten, wie Mindestlänge und Ablaufintervalle.
- g) Es müssen Verfahren vorhanden sein, um verdächtige Konten zu identifizieren und zu kennzeichnen, um ihre unbefugte Nutzung zu verhindern. Diese Verfahren umfassen:
 - i. Benachrichtigung des Systemadministrators und Sperrung des Benutzers oder Eintrag in den Prüfpfad nach einer maximalen Anzahl von drei falschen Authentifizierungsversuchen;
 - ii. Kennzeichnung verdächtiger Konten, bei denen die Authentifizierungsdaten gestohlen worden sein könnten; und
 - iii. Ungültigmachung von Konten und Übertragung kritischer gespeicherter Kontoinformationen auf ein neues Konto.
- h) Alle logischen Zugriffsversuche auf die Systemanwendungen oder Betriebssysteme werden in einem sicheren Protokoll aufgezeichnet.
- i) Die Verwendung von Hilfsprogrammen, die Anwendungs- oder Betriebssystemkontrollen außer Kraft setzen können, muss eingeschränkt und streng kontrolliert werden.
- j) Beschränkungen der Verbindungszeiten, wie z. B. Sitzungszeitlimits, sind zu verwenden, um zusätzliche Sicherheit für Anwendungen mit hohem Risiko, wie z. B. den Fernzugriff, zu gewährleisten.

HINWEIS: Wenn Passwörter als Authentifizierungsdaten genutzt werden, wird für diese eine Länge von mindestens acht Zeichen empfohlen.

B.2.4 Benutzerberechtigung

Das interaktive Spielsystem muss die folgenden Anforderungen an die Benutzerautorisierung erfüllen:

- a) Es wird ein sicherer und kontrollierter Mechanismus eingesetzt, anhand dessen überprüft werden kann, dass der Zugriff auf die kritische Komponente durch autorisiertes Personal bei Bedarf und in regelmäßigen Abständen erfolgt, wie von der Regulierungsbehörde vorgeschrieben.
- b) Werden automatische Verfahren zur Identifizierung von Geräten zur Authentifizierung von Verbindungen von bestimmten Standorten und Geräten verwendet, so sind diese zu dokumentieren und in die Überprüfung der Zugangsrechte und -privilegien einzubeziehen.
- c) Alle vom System zu Identifizierungszwecken übermittelten Berechtigungsinformationen sind zum Zeitpunkt der Anforderung vom System einzuholen und nicht auf der Systemkomponente zu speichern.
- d) Werden Benutzersitzungen für die Autorisierung verfolgt, so sind die Autorisierungsinformationen für die Benutzersitzung immer nach dem Zufallsprinzip im Speicher zu erstellen und nach Beendigung der Benutzersitzung zu entfernen.

B.2.5 Server-Programmierung

Das interaktive Spielsystem muss ausreichend gesichert sein, um zu verhindern, dass vom Benutzer initiierte Programmierfunktionen auf dem Server zu Änderungen an der Datenbank führen können. Es ist jedoch zulässig, dass Netzwerk- oder Systemadministratoren mit ausreichenden Zugriffsrechten autorisierte Wartungsarbeiten an der Netzwerkinfrastruktur oder Fehlerbehebungen bei Anwendungen durchführen. Der Server muss zudem vor der unbefugten Ausführung eines mobilen Codes geschützt sein.

B.2.6 Verifizierungsverfahren

Es müssen Verfahren vorhanden sein, anhand derer überprüft werden kann, ob die kritischen Kontrollprogramm-Komponenten des interaktiven Spielsystems in der Produktionsumgebung mit den von der Regulierungsbehörde genehmigten übereinstimmen.

- a) Die Signaturen der kritischen Kontrollprogramm-Komponenten sind in der Produktionsumgebung nach einem von der Regulierungsbehörde zu genehmigenden Verfahren zu erfassen und durchzuführen:
 - i. bei der Installation/Aktualisierung von Komponenten;
 - ii. beim Einschalten oder bei der Wiederherstellung aus einem abgeschalteten Zustand;
 - iii. mindestens einmal alle 24 Stunden; und
 - iv. bei Bedarf.
- b) Das Verfahren muss einen oder mehrere Analyseschritte umfassen, um die aktuellen Signaturen der kritischen Kontrollprogramm-Komponenten in der Produktionsumgebung mit den

Signaturen der aktuell genehmigten Versionen der kritischen Kontrollprogramm-Komponenten zu vergleichen.

- c) Die Ergebnisse des Verfahrens müssen die aktuellen und die erwarteten Signaturergebnisse enthalten und in einem unveränderlichen Format gespeichert werden, in dem die Überprüfungsergebnisse für die Authentifizierung jedes kritischen Kontrollprogramms im Einzelnen aufgeführt sind:
 - i. in einem Systemprotokoll oder einem Bericht aufgezeichnet werden, der für einen Zeitraum von neunzig Tagen oder nach Maßgabe der Regulierungsbehörde aufbewahrt wird;
 - ii. der Regulierungsbehörde in einem Format zugänglich sein, das die Analyse der Verifizierungsaufzeichnungen durch die Regulierungsbehörde ermöglicht; und
 - iii. Teil der Systemaufzeichnungen sein, die im Falle einer Katastrophe oder eines Geräte- oder Softwareausfalls wiederhergestellt werden müssen.
- d) Jede fehlgeschlagene Verifizierung einer Komponente des Systems erfordert eine Benachrichtigung des Betreibers und der Regulierungsbehörde über die fehlgeschlagene Authentifizierung.
- e) Es muss ein Verfahren vorhanden sein, mit dem auf fehlgeschlagene Authentifizierungen reagiert werden kann, einschließlich der Ermittlung der Fehlerursache und der Durchführung der erforderlichen Korrekturen oder Neuinstallationen in angemessener Zeit.

B.2.7 Elektronisches Dokumentenaufbewahrungssystem

Die in diesem Standard unter „Berichtsanforderungen“ aufgeführten und von der Regulierungsbehörde geforderten Berichte können in einem elektronischen Dokumentenaufbewahrungssystem gespeichert werden, sofern das System:

- a) ordnungsgemäß konfiguriert ist, um die ursprüngliche Version zusammen mit allen nachfolgenden Versionen aufzubewahren, die alle Änderungen an dem Bericht widerspiegeln, wenn die Berichte in einem veränderbaren Format gespeichert sind;
- b) eine eindeutige Signatur für jede Version des Berichts enthält, einschließlich des Originals;
- c) ein vollständiges Protokoll der Änderungen an allen Berichten aufbewahrt und meldet, wer (Benutzerkennung) die Änderungen vorgenommen hat und wann (Datum und Uhrzeit) sie vorgenommen wurden;
- d) eine Methode zur vollständigen Indizierung bietet, um den Bericht leicht aufzufinden und zu identifizieren, einschließlich mindestens der folgenden Angaben (die vom Benutzer eingegeben werden können):
 - i. Datum und Uhrzeit der Erstellung des Berichts;
 - ii. Anwendung oder System, das den Bericht erstellt;
 - iii. Titel und Beschreibung des Berichts;
 - iv. Identifikation des Benutzers, der den Bericht erstellt;
 - v. alle anderen Informationen, die zur Identifizierung des Berichts und seines Zwecks nützlich sein können;
- e) ist so konfiguriert, dass der Zugriff zum Ändern oder Hinzufügen von Berichten zum System durch die logische Sicherheit bestimmter Benutzerkonten eingeschränkt wird;
- f) ist so konfiguriert, dass ein vollständiger Prüfpfad für alle administrativen Benutzeraktivitäten erstellt wird;

- g) ist durch logische Sicherheitsmaßnahmen ordnungsgemäß gesichert (Benutzerkonten mit angemessenem Zugriff, angemessene Protokollierung von Ereignissen, Dokumentation der Versionskontrolle usw.);
- h) ist physisch mit allen anderen kritischen Komponenten des interaktiven Spielsystems gesichert; und
- i) ist so ausgestattet, dass eine Unterbrechung der Berichtsverfügbarkeit und ein Datenverlust durch bewährte Hardware- und Software-Redundanzverfahren und Backup-Prozesse verhindert werden.

B.2.8 Verwaltung von Vermögenswerten

Über alle physischen oder logischen Vermögenswerte, die sensible Informationen enthalten, verarbeiten oder übermitteln, einschließlich derjenigen, die die Betriebsumgebung des Interaktiven Spielsystems und/oder seiner Komponenten bilden, muss Rechenschaft abgelegt werden.

- a) Es müssen Verfahren für das Hinzufügen neuer Vermögenswerte und das Entfernen von Vermögenswerten vorhanden sein.
- b) Die Entsorgung von Vermögenswerten erfolgt sicher und unter Verwendung dokumentierter Verfahren.
- c) Es muss eine Richtlinie über die zulässige Nutzung von Vermögenswerten im Zusammenhang mit dem System und seiner Betriebsumgebung vorhanden sein.
- d) Der festgelegte „Eigentümer“ jedes Vermögenswertes ist verantwortlich für:
 - i. Die Sicherstellung, dass Informationen und Vermögenswerte hinsichtlich ihrer Vertraulichkeit, Integrität, Verantwortlichkeit und Verfügbarkeit angemessen eingestuft sind; und
 - ii. die Festlegung und regelmäßige Überprüfung von Zugriffsbeschränkungen und Klassifizierungen.
- e) Es muss ein Verfahren vorhanden sein, anhand dessen sichergestellt wird, dass mindestens einmal jährlich oder in den von der Regulierungsbehörde geforderten Abständen ein Abgleich zwischen den verbuchten und den tatsächlichen Vermögenswerten erfolgt und im Fall von Abweichungen geeignete Maßnahmen ergriffen werden.
- f) Ein Kopierschutz zur Verhinderung der unbefugten Vervielfältigung oder Änderung von lizenzierter Software kann unter folgenden Voraussetzungen eingerichtet werden:
 - i. Die Methode des Kopierschutzes wird vollständig dokumentiert und dem unabhängigen Testlabor zur Verfügung gestellt, um zu überprüfen, ob der Schutz wie beschrieben funktioniert; oder
 - ii. das Programm oder die Komponente, die für die Durchsetzung des Kopierschutzes verantwortlich ist, kann einzeln nach der von der Regulierungsbehörde genehmigten Methode überprüft werden.
- g) Vor der Entsorgung oder Wiederverwendung sind Vermögenswerten, die Speichermedien enthalten, zu überprüfen, um sicherzustellen, dass lizenzierte Software sowie personenbezogene Daten und andere sensible Informationen entfernt oder sicher überschrieben (d. h. nicht nur gelöscht) wurden.

B.2.9 Register kritischer Vermögenswerte

Ein Register kritischer Vermögenswerte (Critical Asset Register, CAR) wird für alle Vermögenswerte geführt, die die Funktionalität des interaktiven Glücksspielsystems beeinflussen oder einen Einfluss darauf haben, wie personenbezogene Daten und andere sensible Informationen vom System gespeichert/verarbeitet werden. Die Struktur des CAR muss Hardware- und Softwarekomponenten sowie die Beziehungen und Abhängigkeiten zwischen den Komponenten umfassen. Für jeden Vermögenswert sind mindestens die folgenden Daten zu dokumentieren:

- a) Name/Definition jedes Vermögenswerts;
- b) eine eindeutige Kennung, die jedem einzelnen Vermögenswert zugewiesen wird;
- c) eine Versionsnummer des aufgeführten Vermögenswerts;
- d) identifizierende Merkmale des Vermögenswerts (z. B. Systemkomponente, Datenbank, virtuelle Maschine, Hardware);
- e) der für den Vermögenswert verantwortliche „Eigentümer“;
- f) der geografische Standort des Hardwarebestands;
- g) Relevanzcodes für die Rolle des Vermögenswerts bei der Erreichung oder Gewährleistung der folgenden Klassifizierungskriterien:
 - i. Vertraulichkeit von personenbezogenen Daten und anderen sensiblen Informationen (z. B. Identifikations- und Transaktionsdaten);
 - ii. Integrität des Systems, insbesondere jeder Vermögenswert, der sich auf die Funktionalität des Systems auswirkt und/oder einen Einfluss darauf hat, wie personenbezogene Daten und andere sensible Informationen gespeichert und/oder gehandhabt werden;
 - iii. Verfügbarkeit von personenbezogenen Daten und anderen sensiblen Informationen; und
 - iv. Rechenschaftspflicht in Bezug auf Benutzeraktivitäten und wie viel Einfluss der Vermögenswert auf die Benutzeraktivitäten hat.

HINWEIS: Für jedes der oben genannten Klassifizierungskriterien wird ein Relevanzcode von 1, d. h. keine Relevanz (der Vermögenswert kann sich nicht negativ auf die Kriterien auswirken), 2, d. h. eine gewisse Relevanz (der Vermögenswert kann sich auf die Kriterien auswirken), oder 3, d. h. eine erhebliche Relevanz (die Kriterien sind mit dem Vermögenswert verbunden oder von ihm abhängig), vergeben.

B.3 Datenintegrität

B.3.1 Datensicherheit

Der Betreiber muss ein mehrschichtiges Sicherheitskonzept für die Produktionsumgebung bereitstellen, um die sichere Speicherung und Verarbeitung von Daten zu gewährleisten. Das interaktive Spielsystem sollte ein logisches Mittel zur Sicherung von personenbezogenen Daten und anderen sensiblen Informationen, einschließlich Daten der Rechnungsführung, des Berichtswesens, wichtiger Ereignisse oder anderen Spieler- und Spieldaten, gegen Veränderung, Manipulation oder unbefugtem Zugriff bieten.

- a) Es sind geeignete Datenverarbeitungsmethoden zu implementieren, einschließlich der Validierung von Eingaben und der Zurückweisung von beschädigten Daten.
- b) Die Anzahl der Arbeitsplätze, an denen auf kritische Anwendungen oder zugehörige Datenbanken zugegriffen werden kann, ist zu begrenzen.

- c) Für Dateien und Verzeichnisse, die Daten enthalten, ist eine Verschlüsselung oder ein Passwortschutz oder ein gleichwertiger Schutz zu verwenden. Wird keine Verschlüsselung verwendet, so muss der Betreiber die Benutzer daran hindern, den Inhalt solcher Dateien und Verzeichnisse einzusehen, wobei zumindest eine Trennung der Systemaufgaben und -zuständigkeiten sowie die Überwachung und Aufzeichnung des Zugriffs von Personen auf solche Dateien und Verzeichnisse vorzusehen ist.
- d) Der normale Betrieb von Geräten, die Daten enthalten, darf keine Optionen oder Mechanismen aufweisen, die die Daten gefährden könnten.
- e) Kein Gerät darf über einen Mechanismus verfügen, der bei einem Fehler die automatische Löschung der Daten bewirkt.
- f) Jedes Gerät, das Daten in seinem Speicher hält, darf das Entfernen der Informationen nur dann zulassen, wenn es diese Informationen zuvor an die Datenbank oder andere gesicherte Komponenten des Systems übertragen hat.
- g) Personenbezogene Daten und andere sensible Informationen werden in Bereichen des Servers gespeichert, die verschlüsselt und vor unbefugtem Zugriff, sowohl von außen als auch intern, geschützt sind.
- h) Produktionsdatenbanken, die Daten enthalten, müssen sich in Netzwerken befinden, die von den Servern getrennt sind, auf denen etwaige Spielerschnittstellen gehostet werden.
- i) Die Daten müssen jederzeit erhalten werden, unabhängig davon, ob der Server mit Strom versorgt wird.
- j) Die Daten sind so zu speichern, dass sie beim Austausch von Teilen oder Modulen während der normalen Wartung nicht verloren gehen.

B.3.2 Änderung von Daten

Die Änderung jeglicher Daten der Rechnungsführung, des Berichtswesens oder wichtiger Ereignisse darf nicht ohne überwachte Zugangskontrollen erfolgen. Werden Daten geändert, so sind die folgenden Informationen zu dokumentieren oder zu protokollieren:

- a) eindeutige Identifikationsnummer für die Änderung;
- b) geändertes Datenelement;
- c) Wert des Datenelements vor der Änderung;
- d) Wert des Datenelements nach der Änderung;
- e) Uhrzeit und Datum der Änderung; und
- f) Personal, das die Änderung vorgenommen hat (Benutzerkennung).

B.3.3 Häufigkeit der Datensicherung

Die Umsetzung des Sicherungsplans muss mindestens einmal täglich oder nach anderen von der Regulierungsbehörde festgelegten Vorgaben erfolgen, wobei alle Methoden auf Fall-zu-Fall-Basis geprüft werden.

B.3.4 Sicherung von Datenträgern

Prüfprotokolle, Systemdatenbanken und andere personenbezogene Daten oder relevante Spieldaten werden mit angemessenen Schutzmethoden gespeichert. Das interaktive Spielsystem muss so

konzipiert sein, dass die Integrität dieser Daten im Falle eines Ausfalls geschützt ist. Redundante Kopien dieser Daten werden auf dem System aufbewahrt, mit offenem Support zur Sicherung und Wiederherstellung, so dass kein einziger Ausfall eines Teils des Systems zum Verlust oder zur Beschädigung von Daten führen würde.

- a) Die Sicherungskopie muss auf einem nicht-flüchtigen physischen Medium oder einer gleichwertigen architektonischen Implementierung enthalten sein, so dass bei einem Ausfall des primären Speichermediums die Funktionen des Systems und der Prozess der Prüfung dieser Funktionen ohne kritischen Datenverlust fortgesetzt werden können. Werden Festplattenlaufwerke als Speichermedium verwendet, muss die Datenintegrität bei einem Festplattenausfall gewährleistet sein.
- b) Nach Abschluss des Sicherungsvorgangs werden die Speichermedien unverzüglich an einen Ort gebracht, der physisch von dem Ort getrennt ist, an dem sich die zu sichernden Server und Daten befinden (zur vorübergehenden und dauerhaften Speicherung).
 - i. Der Speicherort muss so gesichert sein, dass ein unbefugter Zugriff verhindert wird, und er muss einen angemessenen Schutz bieten, um den dauerhaften Verlust von Daten zu verhindern.
 - ii. Für Sicherungsdateien und Datenwiederherstellungskomponenten gelten mindestens dieselben Sicherheits- und Zugangskontrollen wie für das System.
- c) Wenn die Regulierungsbehörde die Nutzung von Cloud-Plattformen zulässt, kann eine weitere Kopie der in einer Cloud-Plattform gespeicherten Sicherungskopie in einer anderen Cloud-Plattform oder Region gespeichert werden.

B.3.5 Systemausfälle

Das interaktive Spielsystem muss über eine ausreichende Redundanz und Modularität verfügen, so dass beim Ausfall einer einzelnen Komponente oder eines Teils einer Komponente die Funktionen des Systems und der Prozess der Prüfung dieser Funktionen ohne kritischen Datenverlust fortgesetzt werden können. Wenn zwei oder mehr Komponenten miteinander verbunden sind, muss ein Verfahren vorhanden sein, anhand dessen das interaktive Spielsystem und die Komponenten nach der Installation, aber vor dem Einsatz in einer Produktionsumgebung getestet werden können, um folgendes zu überprüfen:

- a) Der Ablauf aller Spielvorgänge zwischen den Komponenten darf durch einen Neustart oder eine Wiederherstellung einer der Komponenten nicht beeinträchtigt werden (z. B. dürfen keine Transaktionen aufgrund der Wiederherstellung der einen oder anderen Komponente verloren gehen oder dupliziert werden); und
- b) nach einem Neustart oder einer Wiederherstellung müssen die Komponenten den Status aller Transaktionen, Daten und Konfigurationen sofort miteinander synchronisieren.

B.3.6 Berücksichtigung von Master-Resets

Der Betreiber muss in der Lage sein, die Situation, in der ein Master-Reset bei einer Komponente, die sich auf den Spielbetrieb auswirkt, aufgetreten ist, zu erkennen und angemessen zu handeln.

B.3.7 Wiederherstellungsanforderungen

Im Falle eines katastrophalen Ausfalls, bei dem das interaktive Spielsystem nicht auf andere Weise neu gestartet werden kann, muss es möglich sein, das System ab dem letzten Sicherungspunkt und vollständig wiederherzustellen. Der Inhalt dieser Sicherheitskopie muss die folgenden kritischen Informationen enthalten, einschließlich, aber nicht beschränkt auf:

- a) die aufgezeichneten Informationen, die im Abschnitt „Zu sichernde Informationen“ aufgeführt sind;
- b) spezifische Informationen über den Standort oder Austragungsort wie Konfiguration, Sicherheitskonten usw.;
- c) aktuelle Systemverschlüsselungscodes; und
- d) alle anderen Systemparameter, Modifikationen, Neukonfigurationen (einschließlich teilnehmender Standorte oder Austragungsorte), Ergänzungen, Zusammenführungen, Löschungen, Anpassungen und Parameteränderungen.

B.3.8 Unterstützung für unterbrechungsfreie Stromversorgung (USV)

Alle Systemkomponenten müssen mit einer ausreichenden Primärstromversorgung ausgestattet sein. Handelt es sich bei dem Server um eine eigenständige Anwendung, so muss er an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen sein, die über eine ausreichende Kapazität verfügt, um ein ordnungsgemäßes Herunterfahren zu ermöglichen und bei einem Stromausfall alle personenbezogenen Daten und anderen sensiblen Informationen beizubehalten. Es ist zulässig, dass das System eine Komponente eines Netzwerks ist, das von einer netzwerkweiten USV unterstützt wird, vorausgesetzt, dass der Server als ein von der USV geschütztes Gerät enthalten ist. Es muss ein Überspannungsschutzsystem vorhanden sein, sofern es nicht in die USV selbst integriert ist.

B.3.9 Geschäftskontinuität und Notfallwiederherstellungsplan

Es muss ein Plan zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung im Katastrophenfall vorhanden sein, um den Spielbetrieb wiederherstellen zu können, wenn die Produktionsumgebung des interaktiven Glücksspielsystems nicht mehr funktionsfähig ist. Ein solcher Plan muss Katastrophen miteinbeziehen, einschließlich, aber nicht beschränkt auf solche, die durch Wetter, Wasser, Überschwemmung, Feuer, Schäden durch verschüttete Flüssigkeiten und Missgeschicke, böswillige Zerstörung, terroristische oder kriegerische Handlungen sowie Unwägbarkeiten wie Streiks, Epidemien, Pandemien usw. verursacht werden. Der Plan zur Aufrechterhaltung des Geschäftsbetriebs und zur Wiederherstellung im Katastrophenfall muss:

- a) die Methode zur Speicherung von personenbezogenen Daten und anderen sensiblen Informationen, einschließlich Spieldaten, umfassen, um den Verlust zu minimieren. Wenn eine asynchrone Replikation verwendet wird, muss die Methode zur Wiederherstellung von Informationen beschrieben oder der potenzielle Verlust von Informationen dokumentiert werden;
- b) müssen die Umstände, unter denen das Verfahren angewandt wird, beschrieben werden;

- c) muss die Einrichtung eines Wiederherstellungsstandorts vorgesehen sein, der physisch vom Produktionsstandort getrennt ist. Die Nutzung von Cloud-Plattformen für diesen Zweck ist auf einer Fall-zu-Fall-Basis zu prüfen;
- d) müssen Wiederherstellungsleitfäden enthalten sein, die die technischen Schritte beschreiben, die zur Wiederherstellung der Spielfunktionalität am Wiederherstellungsstandort erforderlich sind; und
- e) müssen Verfahren vorgesehen sein, die für die Wiederaufnahme des administrativen Spielbetriebs nach der Aktivierung des wiederhergestellten Systems erforderlich sind, und zwar für eine Reihe von Szenarien, die für den betrieblichen Kontext des Systems geeignet sind.

HINWEIS: Die Entfernung zwischen den beiden Standorten sollte auf der Grundlage potenzieller Umweltbedrohungen und -gefahren, Stromausfälle und anderer Störungen bestimmt werden, jedoch sollten auch die potenziellen Schwierigkeiten bei der Datenreplikation sowie die Möglichkeit, den Wiederherstellungsstandort innerhalb einer angemessenen Zeit zu erreichen (Wiederherstellungszeitvorgabe), berücksichtigt werden.

B.4 Kommunikation

B.4.1 Allgemeines

In diesem Abschnitt werden die verschiedenen drahtgebundenen und drahtlosen Kommunikationsmethoden erörtert, einschließlich der Kommunikation über das Internet oder ein öffentliches Netz oder ein Netz eines Drittanbieters, sofern dies von der Regulierungsbehörde zugelassen ist.

B.4.2 Konnektivität

Nur autorisierte Geräte dürfen die Kommunikation zwischen kritischen Komponenten des Systems herstellen. Das interaktive Spielsystem muss eine Methode bieten, um:

- a) kritische Komponenten an- und abzumelden;
- b) bestimmte kritische Komponenten zu aktivieren und deaktivieren;
- c) sicherzustellen, dass nur angemeldete und aktivierte kritische Komponenten am Spielbetrieb teilnehmen können; und
- d) sicherzustellen, dass der Standardzustand für kritische Komponenten nicht angemeldet und deaktiviert ist.

B.4.3 Kommunikationsprotokoll

Jede Komponente des interaktiven Spielsystems muss so funktionieren, wie es in einem dokumentierten sicheren Kommunikationsprotokoll angegeben ist.

- a) Alle Protokolle verwenden Kommunikationstechniken mit geeigneten Fehlererkennungs- und Wiederherstellungsmechanismen, die das Eindringen, Stören, Abhören und Manipulieren verhindern sollen. Alle alternativen Implementierungen werden auf Fall-zu-Fall-Basis geprüft und von der Regulierungsbehörde genehmigt.

- b) Die gesamte Datenkommunikation, die für die Verwaltung von Spielen oder Spielerkonten entscheidend ist, muss verschlüsselt und authentifiziert werden.
- c) Die Kommunikation über das sichere Netz ist nur zwischen zugelassenen kritischen Komponenten möglich, die im Netz registriert und als gültig authentifiziert wurden. Unerlaubte Kommunikation mit Komponenten und/oder Zugangspunkten ist nicht zulässig.
- d) Die Kommunikation muss gesichert sein, um gegen alle möglichen Angriffe auf manipulierte Nachrichten immun zu sein.
- e) Nach einer Systemunterbrechung oder -abschaltung darf die Kommunikation mit allen für den Systembetrieb erforderlichen Komponenten erst dann hergestellt und authentifiziert werden, wenn die Routine zur Wiederaufnahme des Programms, einschließlich etwaiger Selbsttests, erfolgreich abgeschlossen ist.

B.4.4 Kommunikation über das Internet/öffentliche Netze

Die Kommunikation zwischen Systemkomponenten, einschließlich Remote-Spieler-Geräten, die über das Internet/öffentliche Netze erfolgt, muss durch Verschlüsselung der Datenpakete oder durch Verwendung eines sicheren Kommunikationsprotokolls gesichert werden, um die Integrität und Vertraulichkeit der Übertragung zu gewährleisten. Personenbezogene Daten, sensible Informationen, Wetteinsätze, Ergebnisse, Finanzinformationen und Spielertransaktionsdaten müssen über das Internet/öffentliche Netze stets verschlüsselt und vor unvollständigen Übertragungen, Fehlleitungen, unbefugter Änderung, Offenlegung, Vervielfältigung oder Wiederholung geschützt werden.

B.4.5 Kommunikation über drahtlose lokale Netzwerke (WLAN)

Kommunikation über ein drahtloses lokales Netzwerk (WLAN), die von der Regulierungsbehörde erlaubt ist, muss den geltenden rechtlichen Anforderungen für drahtlose Geräte und die Netzwerksicherheit entsprechen. In Ermangelung spezifischer gesetzlicher Normen sind die „Anforderungen an drahtlose Geräte“ und die „Anforderungen an die Sicherheit drahtloser Netze“ der *GLI-26* „Standards für drahtlose Systeme“ anzuwenden.

HINWEIS: Für Betreiber ist es zwingend erforderlich, ihre internen Kontrollstrategien und -verfahren zu überprüfen und aktualisieren, um zu gewährleisten, dass das Netz sicher ist und Bedrohungen und Schwachstellen entsprechend angegangen werden. Eine regelmäßige Inspektion und Überprüfung der Integrität des WLAN wird empfohlen.

B.4.6 Verwaltung der Netzwerksicherheit

Die Netze sind logisch so zu trennen, dass auf einer Netzverbindung kein Netzverkehr stattfindet, der nicht von den Hosts auf dieser Verbindung abgewickelt werden kann. Es gelten die folgenden Anforderungen:

- a) Alle Netzwerkverwaltungsfunktionen müssen alle Benutzer im Netzwerk authentifizieren und die gesamte Netzwerkverwaltungs-kommunikation verschlüsseln.
- b) Der Ausfall eines einzelnen Elements darf nicht zu einer Dienstverweigerung (Denial of Service) führen.

- c) Es muss ein Intrusion Detection System/Intrusion Prevention System (IDS/IPS) installiert sein, das eine oder mehrere Komponenten umfasst, die sowohl interne als auch externe Kommunikation abhören und Folgendes erkennen oder verhindern können:
 - i. Distributed-Denial-of-Service-Angriffe;
 - ii. Shellcode, der das Netz durchdringt;
 - iii. Address Resolution Protocol (ARP) Spoofing; und
 - iv. andere Anzeichen für „Man-In-The-Middle“-Angriffe, um bei Entdeckung die Kommunikation sofort zu unterbrechen.
- d) Zusätzlich zu den Anforderungen unter c) muss ein in einem WLAN installiertes IDS/IPS in der Lage sein:
 - i. das Netz mindestens vierteljährlich oder nach Vorgabe der Regulierungsbehörde auf unautorisierte oder unberechtigte Zugangspunkte oder Geräte, die mit einem Zugangspunkt des Netzes verbunden sind, zu überprüfen;
 - ii. automatisch alle nicht autorisierten oder unseriösen Geräte, die mit dem System verbunden sind, zu deaktivieren; und
 - iii. ein Protokoll aller drahtlosen Zugriffe für mindestens die letzten neunzig Tage oder wie von der Regulierungsbehörde festgelegt zu führen. Dieses Protokoll muss vollständige und umfassende Informationen über alle beteiligten drahtlosen Geräte enthalten und mit allen anderen Netzwerkgeräten am Standort oder Austragungsort abgeglichen werden können.
- e) Die Netzwerkkommunikationsgeräte (Network Communication Equipment, NCE) müssen die folgenden Anforderungen erfüllen:
 - i. Netzwerkkommunikationsgeräte müssen so konstruiert sein, dass sie gegen physische Beschädigung der Hardware oder Beschädigung der enthaltenen Firmware/Software durch normalen Gebrauch resistent sind;
 - ii. Netzwerkkommunikationsgeräte müssen physisch gegen unbefugten Zugriff gesichert sein;
 - iii. die Systemkommunikation über Netzwerkkommunikationsgeräte muss logisch gegen unbefugten Zugriff gesichert sein; und
 - iv. Netzwerkkommunikationsgeräte mit begrenztem eingebautem Speicher müssen, wenn das Prüfprotokoll voll ist, die gesamte Kommunikation deaktivieren oder die Protokolle auf einen speziellen Protokollserver auslagern.
- f) Alle Eingangs- und Ausgangspunkte des Netzwerkes müssen identifiziert, verwaltet, kontrolliert und rund um die Uhr überwacht werden. Darüber hinaus:
 - i. sind alle Netzknotenpunkte, Dienste und Verbindungsports zu sichern, um den unbefugten Zugang zum Netz zu verhindern; und
 - ii. nicht genutzte Dienste und nicht benötigte Ports sind nach Möglichkeit entweder physisch zu blockieren oder per Software zu deaktivieren.
- g) In Cloud- und virtualisierten Umgebungen dürfen redundante Serverinstanzen nicht unter demselben Hypervisor laufen. Darüber hinaus:
 - i. darf jede Serverinstanz nur eine Funktion ausüben; und
 - ii. werden alternative, gleichwertige Sicherheitsmechanismen im Zuge des technischen Fortschritts in Betracht gezogen.
- h) Zustandslose Protokolle, wie z. B. UDP (User Datagram Protocol), dürfen nicht für sensible Informationen ohne zustandsabhängigen Transport verwendet werden. Es ist zu beachten, dass das HTTP (Hypertext Transport Protocol) zwar technisch gesehen zustandslos ist, aber wenn es auf einem zustandsbehafteten TCP (Transmission Control Protocol) läuft, dies zugelassen ist.
- i) Alle Änderungen an der Netzinfrastruktur (z. B. an der Konfiguration der

Netzkommunikationsgeräte) sind zu protokollieren.

- j) Auf dem System sind Virens Scanner und/oder Virenerkennungsprogramme zu installieren. Diese Programme müssen regelmäßig aktualisiert werden, um Virenstämme zu erkennen.
- k) Der Betreiber muss das System und das Netz überwachen, um Cyberangriffe zu verhindern, zu erkennen, zu entschärfen und darauf zu reagieren.

B.4.7 Aktive und passive Angriffe

Es müssen geeignete Maßnahmen vorhanden sein, um gängige aktive und passive technische Angriffe zu erkennen, zu verhindern, zu entschärfen und darauf zu reagieren. Der Betreiber muss über ein festgelegtes Verfahren verfügen, um Informationen über Cyber-Bedrohungen zu sammeln und angemessen darauf zu reagieren.

B.4.8 Mobile Datenverarbeitung und Kommunikation

Es muss eine offizielle Richtlinie vorhanden sein, und es müssen geeignete Sicherheitsmaßnahmen ergriffen werden, um sich gegen die Risiken der Nutzung mobiler Computer- und Kommunikationseinrichtungen zu schützen. Telearbeit ist nur unter Umständen zulässig, unter denen die Sicherheit des Endpunkts gewährleistet werden kann.

B.5 Drittdienstleister

B.5.1 Kommunikation mit Drittanbietern

Für die Kommunikation mit Drittanbietern, z. B. für Treueprogramme für Spielteilnehmer, Zahlungsdienste (Finanzinstitute, Zahlungsabwickler usw.), Standortdienste, Informationssicherheitsdienste, Cloud-Dienste, Live-Spiel-Dienste und Identitätsüberprüfungsdienste, gelten die folgenden Anforderungen:

- a) Das interaktive Spielsystem muss in der Lage sein, mit Drittanbietern unter Verwendung von Verschlüsselung und starker Authentifizierung sicher zu kommunizieren.
- b) Alle Anmeldevorgänge, an denen Drittanbieter beteiligt sind, müssen in einer Audit-Datei erfasst werden.
- c) Die Kommunikation mit Drittanbietern darf die normalen Funktionen des interaktiven Spielsystems nicht stören oder beeinträchtigen.
 - i. Die Daten von Drittanbietern dürfen die Kommunikation der Spielteilnehmer nicht beeinträchtigen.
 - ii. Drittanbieter müssen sich in einem segmentierten Netz befinden, das von den Netzsegmenten getrennt ist, über die Spielerverbindungen laufen.
 - iii. Der Spielbetrieb muss auf allen Netzwerkverbindungen mit Ausnahme derjenigen innerhalb der Produktionsumgebung deaktiviert sein.
 - iv. Das System darf keine Datenpakete von Drittanbietern direkt an die Produktionsumgebung weiterleiten und umgekehrt.
 - v. Das System darf nicht als IP-Router zwischen der Produktionsumgebung und Drittanbietern fungieren.

B.5.2 Dienstleistungen von Drittanbietern

Die Sicherheitsaufgaben und -zuständigkeiten von Drittanbietern müssen entsprechend den Anforderungen der Regulierungsbehörde definiert und dokumentiert werden. Der Betreiber muss über Strategien und Verfahren verfügen, um sie zu verwalten und ihre Einhaltung der einschlägigen Sicherheitsanforderungen zu überwachen.

- a) Vereinbarungen mit Drittanbietern, die den Zugriff auf das System und/oder seine Komponenten, die Verarbeitung, die Kommunikation oder die Verwaltung des Systems und/oder seiner Komponenten oder die Hinzufügung von Produkten oder Diensten zu dem System und/oder seinen Komponenten betreffen, müssen alle relevanten Sicherheitsanforderungen abdecken.
- b) Die von den Drittanbietern erbrachten Dienste, Berichte und Aufzeichnungen werden jährlich oder nach Aufforderung durch die Regulierungsbehörde überwacht und überprüft.
- c) Änderungen bei der Erbringung von Dienstleistungen durch Drittanbieter, einschließlich der Beibehaltung und Verbesserung bestehender Sicherheitsstrategien, -verfahren und -kontrollen, sind unter Berücksichtigung der Kritikalität der betroffenen Systeme und Prozesse und der Neubewertung der Risiken zu verwalten.
- d) Die Zugriffsrechte von Drittanbietern auf das System und/oder seine Komponenten sind bei Beendigung ihres Vertrags oder ihrer Vereinbarung aufzuheben oder bei Änderungen anzupassen.

B.5.3 Datenverarbeitung durch Dritte

Unbefugte Drittanbieter müssen daran gehindert werden, personenbezogene Daten und andere sensible Informationen einzusehen oder zu verändern. Werden personenbezogene Daten und andere sensible Informationen mit Drittanbietern geteilt, müssen förmliche Datenverarbeitungsvereinbarungen bestehen, in denen die Rechte und Pflichten jeder Partei in Bezug auf den Schutz der personenbezogenen Daten und anderer sensibler Informationen festgelegt sind. In jeder Datenverarbeitungsvereinbarung ist Folgendes festzuhalten:

- a) Gegenstand und Dauer der Verarbeitung;
- b) Art und Zweck der Verarbeitung;
- c) Art der zu verarbeitenden Daten;
- d) Art der Datenspeicherung;
- e) Einzelheiten zur Datensicherheit;
- f) Mittel zur Übermittlung der Daten von einer Organisation zur anderen;
- g) Mittel zum Abrufen von Daten über bestimmte Personen;
- h) Methode zur Gewährleistung der Einhaltung eines Aufbewahrungszeitplans;
- i) Mittel zur Löschung oder Entsorgung der Daten und
- j) die Datenkategorien.

B.6 Technische Kontrollen

B.6.1 Anforderungen an den Domain Name Service (DNS)

Die folgenden Anforderungen gelten für die Server, die zur Auflösung von öffentlichen oder externen Domain Name Service (DNS)-Anfragen in Verbindung mit dem interaktiven Spielsystem verwendet werden.

- a) Der Betreiber muss einen sicheren primären DNS-Server und einen sicheren sekundären DNS-Server verwenden, die logisch und physisch voneinander getrennt sind.
- b) Der primäre DNS-Server muss sich physisch in einem sicheren Rechenzentrum oder auf einem virtualisierten Host in einem entsprechend gesicherten Hypervisor oder einem gleichwertigen System befinden.
- c) Der logische und physische Zugang zu dem/den DNS-Server(n) ist auf befugtes Personal zu beschränken.
- d) Zonenübertragungen an beliebige Hosts sind nicht zulässig.
- e) Es muss eine Methode zur Verhinderung von Cache Poisoning, wie DNS Security Extensions (DNSSEC), vorhanden sein.
- f) Es muss ein Multifaktor-Authentifizierungsverfahren vorhanden sein.
- g) Es muss ein Registry Lock vorhanden sein, so dass jeder Antrag auf Änderung des DNS-Servers/der DNS-Server manuell überprüft werden muss.

B.6.2 Kryptographische Maßnahmen

Es wird eine Strategie für den Einsatz kryptografischer Maßnahmen zum Schutz von Informationen entwickelt und umgesetzt.

- a) Personenbezogene Daten und andere sensible Informationen sind zu verschlüsseln, wenn sie ein Netz mit geringerem Vertrauensniveau durchlaufen. Die Verschlüsselung gilt auch für personenbezogene Daten und andere sensible Informationen, die auf tragbaren Computersystemen (z.B. Laptops, USB-Geräten usw.) gespeichert sind.
- b) Für Daten, die nicht verborgen werden müssen, aber zu authentifizieren sind, muss eine Technik zur Authentifizierung von Mitteilungen verwendet werden.
- c) Zur Authentifizierung ist ein Sicherheitszertifikat einer zugelassenen Organisation zu verwenden, das Informationen über den Eigentümer, den Aussteller, das Gültigkeitsdatum, eine eindeutige Seriennummer oder eine andere eindeutige Kennung enthält, die zur Überprüfung des Inhalts des Zertifikats verwendet werden kann.
- d) Der Grad der verwendeten Verschlüsselung muss der Sensibilität der Daten angemessen sein.
- e) Die Verwendung von Verschlüsselungsalgorithmen ist regelmäßig zu überprüfen, um sicherzustellen, dass die aktuellen Verschlüsselungsalgorithmen sicher sind.
- f) Die Verschlüsselungsmethode muss die Verwendung verschiedener Verschlüsselungscodes umfassen, so dass Verschlüsselungsalgorithmen geändert oder ersetzt werden können, um Schwachstellen zu beheben, sobald dies praktisch möglich ist. Andere Methoden sind auf einer Fall-zu-Fall-Basis zu prüfen.
- g) Die Verschlüsselungscodes werden auf einem sicheren und redundanten Speichermedium gespeichert, nachdem sie selbst mit einer anderen Verschlüsselungsmethode und/oder unter Verwendung eines anderen Verschlüsselungscodes verschlüsselt wurden.

B.6.3 Verwaltung von Verschlüsselungscodes

Die Verwaltung der Verschlüsselungscodes erfolgt nach festgelegten Verfahren, die vom Betreiber und/oder der Regulierungsbehörde festgelegt werden und Folgendes umfassen:

- a) Beschaffung oder Erzeugung von Verschlüsselungscodes und deren sichere Aufbewahrung in einer Weise, die den Zugriff einschränkt;
- b) gegebenenfalls Verwaltung des Ablaufs von Verschlüsselungscodes;
- c) Widerruf von Verschlüsselungscodes;
- d) sichere Änderung des aktuellen Verschlüsselungscodesatzes; und
- e) Wiederherstellung von Daten, die mit einem widerrufenen oder abgelaufenen Verschlüsselungscodesatz verschlüsselt wurden, und zwar für einen festgelegten Zeitraum nach dem Ungültigwerden des Verschlüsselungscodes.

B.6.4 Absicherung kritischer Komponenten

Die Konfigurationsverfahren für kritische Komponenten müssen alle bekannten Sicherheitslücken abdecken und mit den in der Branche anerkannten bewährten Verfahren zur Systemabsicherung übereinstimmen. Die Angemessenheit und Wirksamkeit der zur Absicherung kritischer Komponenten ergriffenen Maßnahmen ist regelmäßig zu bewerten, und gegebenenfalls sind Änderungen zur Verbesserung der Absicherung vorzunehmen. Diese Konfigurationsverfahren müssen Folgendes umfassen:

- a) Alle standardmäßigen Konfigurationsparameter sind aus allen Komponenten zu entfernen, bei denen ein Sicherheitsrisiko besteht;
- b) pro Server ist nur eine primäre Funktion zu implementieren, um zu verhindern, dass Funktionen, die unterschiedliche Sicherheitsstufen erfordern, auf demselben Server nebeneinander bestehen;
- c) für alle erforderlichen Dienste, Protokolle oder Hintergrundprogramme, die als unsicher gelten, sind zusätzliche Sicherheitsfunktionen zu implementieren;
- d) die Sicherheitsparameter des Systems sind so zu konfigurieren, dass ein Missbrauch verhindert wird; und
- e) alle unnötigen Funktionen sind zu entfernen, z. B. Skripte, Treiber, Funktionen, Subsysteme, Dateisysteme und unnötige Webserver.

B.6.5 Erstellung und Speicherung von Protokollen

Es müssen Verfahren zur zentralen Überwachung und Verwaltung von Nutzeraktivitäten, Ausnahmen und Informationssicherheitsereignissen vorhanden sein. Die Protokolle, in denen diese Punkte aufgezeichnet werden, müssen:

- a) für jede kritische Komponente des Systems erstellt werden, um Anomalien, Fehler und Warnungen zu überwachen und zu beheben;
- b) für einen angemessenen Zeitraum aufbewahrt werden, um künftige Untersuchungen und die Überwachung der Zugangskontrolle zu ermöglichen;
- c) vor Manipulationen und unbefugtem Zugriff geschützt werden; und
- d) in regelmäßigen Abständen anhand eines dokumentierten Verfahrens überprüft werden. Über jede Überprüfung ist ein Protokoll zu führen.

B.7 Fernzugriff und Firewalls

B.7.1 Sicherheit des Fernzugriffs

Unter Fernzugriff versteht man jeden Zugriff von außerhalb des Systems oder Systemnetzes, einschließlich des Zugriffs von anderen Netzen innerhalb desselben Standorts oder Austragungsortes. Der Fernzugriff ist nur zulässig, wenn er von der Regulierungsbehörde genehmigt wurde und muss:

- a) über eine gesicherte Methode erfolgen, z. B. über ein Multifaktor-Authentifizierungsverfahren;
- b) die Möglichkeit bieten, deaktiviert zu werden;
- c) nur die von der Firewall-Anwendung und den Systemeinstellungen zugelassenen Fernverbindungen zulassen;
- d) auf die Anwendungsfunktionen beschränkt sein, die für die Benutzer zur Erfüllung ihrer Aufgaben erforderlich sind:
 - i. Es sind keine nicht autorisierten Funktionen zur Fernverwaltung von Benutzern (Hinzufügen von Benutzern, Ändern von Berechtigungen usw.) zulässig; und
 - ii. unbefugter Zugriff auf das Betriebssystem oder auf eine Datenbank mit Ausnahme des Abrufs von Informationen über bestehende Funktionen ist verboten.

HINWEIS: Die Sicherheit des Fernzugriffs wird auf Fall-zu-Fall-Basis in Verbindung mit der Implementierung der aktuellen Technologie und der Genehmigung durch die Regulierungsbehörde überprüft.

B.7.2 Fernzugriffsverfahren durch Anbieter

Es ist ein Verfahren für einen streng kontrollierten Fernzugriff einzurichten. Es wird anerkannt, dass der Anbieter bei Bedarf aus der Ferne auf das System und die zugehörigen Komponenten zugreifen kann, um das Produkt und die Benutzer zu unterstützen oder Aktualisierungen/Upgrades vorzunehmen, soweit dies von der Aufsichtsbehörde und dem Betreiber gestattet ist. Dieser Fernzugriff erfolgt über eigens für diesen Zweck reservierte Benutzerkonten, die:

- a) vom Betreiber ständig überwacht werden,
- b) bei Nichtgebrauch deaktiviert sind und
- c) durch logische Sicherheitskontrollen so eingeschränkt sind, dass nur auf die für das Produkt und die Benutzerunterstützung oder die Bereitstellung von Aktualisierungen/Upgrades erforderlichen Anwendungen und/oder Datenbanken zugegriffen werden kann.

B.7.3 Aktivitätsprotokoll für den Fernzugriff

Die Fernzugriffsanwendung führt ein automatisch aktualisiertes Aktivitätsprotokoll, in dem alle Fernzugriffsinformationen enthalten sind. Diese Informationen umfassen:

- a) Identifizierung des/der Benutzer(s), der/die den Fernzugriff durchgeführt und/oder autorisiert hat/haben;
- b) Remote-IP-Adressen, Portnummern, Protokolle und, sofern möglich, MAC-Adressen;
- c) Uhrzeit und Datum des Verbindungsaufbaus und Dauer der Verbindung; und
- d) Aktivität während der Anmeldung, einschließlich der spezifischen Bereiche, auf die zugegriffen wurde, und der vorgenommenen Änderungen.

HINWEIS: Dieses Aktivitätsprotokoll wird regelmäßig auf Verlangen des Betreibers und/oder der Regulierungsbehörde überprüft.

B.7.4 Firewalls

Die gesamte Kommunikation, einschließlich des Fernzugriffs, muss mindestens eine zugelassene Firewall auf Anwendungsebene passieren. Dies gilt auch für Verbindungen zu und von systemfremden Hosts, die vom Betreiber verwendet werden.

- a) Die Firewall muss sich an der Grenze zwischen zwei unterschiedlichen Sicherheitsdomänen befinden.
- b) Ein Gerät, das sich in derselben Broadcast-Domäne wie der Systemhost befindet, darf nicht über eine Einrichtung verfügen, die es ermöglicht, einen alternativen Netzwerkpfad unter Umgehung der Firewall einzurichten.
- c) Jeder alternative Netzwerkpfad, der zu Redundanzzwecken besteht, muss auch durch mindestens eine Firewall auf Anwendungsebene führen.
- d) Nur Firewall-bezogene Anwendungen dürfen sich auf der Firewall befinden.
- e) Auf der Firewall darf nur eine begrenzte Anzahl von Benutzerkonten vorhanden sein (z. B. nur Netz- oder Systemadministratoren).
- f) Die Firewall muss alle Verbindungen abweisen, die nicht ausdrücklich genehmigt wurden.
- g) Die Firewall muss alle Verbindungen von Zielen abweisen, die sich nicht in dem Netz befinden können, aus dem die Nachricht stammt (z. B. RFC1918-Adressen auf der öffentlichen Seite einer Internet-Firewall).
- h) Die Firewall darf den Fernzugriff nur mit einer Verschlüsselung zulassen, die den aktuellen Industriestandards wie ISO/IEC 19790, FIPS 140-2 oder gleichwertigen Standards entspricht.

B.7.5 Firewall-Prüfprotokolle

Firewalls, die zum Schutz der Produktionsumgebung eingesetzt werden, müssen in der Lage sein, Audit-Informationen entsprechend zu protokollieren, so dass diese Informationen vor Verlust oder Veränderung geschützt sind. Zu diesen Informationen gehören die folgenden:

- a) alle Änderungen an der Konfiguration der Firewall;
- b) alle erfolgreichen und erfolglosen Verbindungsversuche durch die Firewall; und
- c) die Quell- und Ziel-IP-Adressen, Portnummern, Protokolle und, falls möglich, MAC-Adressen.

HINWEIS: Ein konfigurierbarer Parameter „Erfolgreiche Verbindungsversuche“ kann verwendet werden, um weitere Verbindungsanfragen zu verweigern, wenn der vordefinierte Schwellenwert überschritten wird. Der Systemadministrator ist ebenfalls zu benachrichtigen.

B.8 Änderungsmanagement

B.8.1 Allgemeines

Die Regulierungsbehörde wählt eine Richtlinie für das Änderungsmanagement für den Umgang mit Aktualisierungen des interaktiven Glücksspielsystems und seiner Komponenten auf der Grundlage der Neigung zu häufigen System-Upgrades und der gewählten Risikotoleranz. Für Systeme, die häufige Updates erfordern, kann ein risikobasiertes Änderungsmanagementprogramm eingesetzt werden, um eine größere Effizienz bei der Bereitstellung von Updates zu gewährleisten. Risikobasierte Richtlinien für das Änderungsmanagement umfassen in der Regel eine Kategorisierung der vorgeschlagenen Änderungen auf der Grundlage der regulatorischen Auswirkungen und legen für jede Kategorie entsprechende Zertifizierungsverfahren fest. Das unabhängige Prüflabor bewertet das System und künftige Änderungen in Übereinstimmung mit dem von der Regulierungsbehörde gewählten Richtlinie für das Änderungsmanagement.

B.8.2 Verfahren zur Kontrolle von Programmänderungen

Die Verfahren zur Kontrolle von Programmänderungen müssen so beschaffen sein, dass sichergestellt ist, dass nur genehmigte Programmversionen in der Produktionsumgebung implementiert werden. Diese Änderungskontrollen müssen Folgendes umfassen:

- a) eine geeignete Softwareversionskontrolle oder ein entsprechender Mechanismus für alle Softwarekomponenten, Quellcode und binäre Kontrollen;
- b) Aufzeichnungen über alle Neuinstallationen und/oder Änderungen am System, einschließlich:
 - i. das Datum der Installation oder Änderung;
 - ii. Einzelheiten über den Grund oder die Art der Installation oder Änderung, z. B. neue Software, Serverreparatur, wesentliche Konfigurationsänderungen;
 - iii. die zu ändernde(n) Komponente(n) einschließlich der eindeutigen Identifikationsnummer aus dem Register kritischer Vermögenswerte, Versionsinformationen und, falls es sich bei der zu ändernden Komponente um Hardware handelt, den physischen Standort dieser Komponente;
 - iv. die Identität des/der Benutzer(s), der/die die Installation oder Änderung vornimmt/vornehmen;
 - v. die Identität des/der Benutzer(s), der/die für die Genehmigung der Installation oder Änderung verantwortlich ist/sind;
- c) eine Strategie für den Fall, dass die Installation fehlschlägt oder ein Problem mit einer oder mehreren im Rahmen der Richtlinie für das Änderungsmanagement durchgeführten Änderungen auftritt:
 - i. Wenn eine externe Partei, wie z. B. ein App-Store, am Freigabeprozess beteiligt ist, muss diese Strategie die Verwaltung von Freigaben durch die externe Partei abdecken. Bei dieser Strategie kann die Schwere des Problems berücksichtigt werden;
 - ii. andernfalls muss diese Strategie die Rückkehr zur letzten Implementierung (Rollback-Plan) umfassen, einschließlich vollständiger Sicherungskopien früherer Softwareversionen und eines Tests des Rollback-Plans vor der Implementierung in die Produktionsumgebung;
- d) eine Richtlinie, die sich mit Änderungsverfahren für Notfälle befasst;

- e) Verfahren für das Testen und die Migration von Änderungen, einschließlich der Identifizierung von autorisiertem Personal zur Abzeichnung vor der Freigabe;
- f) Aufgabentrennung innerhalb des Freigabeprozesses; und
- g) Verfahren, die gewährleisten, dass die technische Dokumentation und die Benutzerdokumentation als Folge einer Änderung aktualisiert werden.

B.8.3 Systementwicklungszyklus

Die Beschaffung und Entwicklung neuer Software erfolgt nach festgelegten Prozessen, die vom Betreiber und/oder der Regulierungsbehörde festgelegt werden.

- a) Die Produktionsumgebung muss logisch und physisch von der Entwicklungs- und Testumgebung getrennt sein. Bei der Verwendung von Cloud-Plattformen darf keine direkte Verbindung zwischen der Produktionsumgebung und einer anderen Umgebung bestehen.
- b) Gegebenenfalls ist die Übertragung von Zuständigkeiten zwischen dem Betreiber und/oder dem Anbieter festzulegen.
- c) Es muss eine dokumentierte Methode zur sicheren Entwicklung von Software vorhanden sein:
 - i. Befolgung von Industriestandards und/oder bewährten Verfahren für die Programmierung und
 - ii. Einbeziehung der Informationssicherheit während des gesamten Lebenszyklus.
- d) Die dokumentierte Testmethodik muss Bestimmungen enthalten, die:
 - i. gewährleisten, dass die Testsoftware nicht in der Produktionsumgebung eingesetzt wird; und
 - ii. die Verwendung tatsächlicher personenbezogener Daten und anderer sensibler Informationen oder anderer Produktionsrohdaten bei den Tests verhindern.
- e) Die gesamte Dokumentation zur Software- und Anwendungsentwicklung muss verfügbar sein und für die Dauer des Lebenszyklus aufbewahrt werden.

B.8.4 Patches

Der Betreiber muss über eine mit der Regulierungsbehörde vereinbarte Patching-Richtlinie verfügen, unabhängig davon, ob sie vom Betreiber oder von einem Drittanbieter entwickelt und unterstützt wird. Alle Patches sollten nach Möglichkeit in einer Entwicklungs- und Testumgebung getestet werden, die genauso konfiguriert ist wie die angestrebte Produktionsumgebung. In Fällen, in denen die Patch-Tests nicht rechtzeitig und gründlich durchgeführt werden können, um die Zeitvorgaben für den Schweregrad der Warnung einzuhalten, und wenn die Regulierungsbehörde dies genehmigt, sollten die Patch-Tests risikobasiert durchgeführt werden, entweder durch Isolierung oder Entfernung der nicht getesteten Komponente aus dem Netz oder durch Anwendung des Patches und nachträglicher Tests.

B.9 Sicherheitstechnische Überprüfung

B.9.1 Regelmäßige Sicherheitstests

Jährlich oder auf Verlangen der Regulierungsbehörde werden technische Sicherheitstests der Produktionsumgebung durchgeführt, um zu gewährleisten, dass keine Schwachstellen bestehen, die die Sicherheit und den Betrieb des interaktiven Spielsystems gefährden.

- a) Diese Tests bestehen aus einer Methode zur Bewertung der Sicherheit mittels einer Angriffssimulation durch einen Dritten nach einer bekannten Methodik, und die Analyse der Schwachstellen besteht in der Identifizierung und passiven Quantifizierung der potenziellen Risiken des Systems.
- b) Unbefugte Zugriffsversuche werden bis zur höchstmöglichen Zugriffsstufe durchgeführt und mit und ohne verfügbare Authentifizierungsdaten abgeschlossen (White-Box/Black-Box-Tests). Dies ermöglicht eine Bewertung von Betriebssystemen und Hardwarekonfigurationen, einschließlich, aber nicht beschränkt auf:
 - i. UDP/TCP-Port-Scans;
 - ii. Stack-Fingerprinting und TCP-Sequenzvorhersage zur Identifizierung von Betriebssystemen und Diensten;
 - iii. Banner-Grabbing für den öffentlichen Dienst;
 - iv. Web-Scanning unter Verwendung von HTTP- und HTTPS-Schwachstellen-Scannern; und
 - v. Scannen von Routern mit BGP (Border Gateway Protocol), BGMP (Border Gateway Multicast Protocol) und SNMP (Simple Network Management Protocol).
- c) Nach Abschluss ist dem Betreiber und/oder der Regulierungsbehörde ein Bericht über die Bewertungen vorzulegen, der Folgendes enthalten muss:
 - i. Umfang der Überprüfung;
 - ii. Name und Firmenzugehörigkeit der Person/en, die die Bewertung durchgeführt hat/haben;
 - iii. Datum der Bewertung;
 - iv. Ergebnisse;
 - v. ggf. empfohlene Abhilfemaßnahmen; und
 - vi. Antwort des Betreibers auf die Ergebnisse und empfohlenen Abhilfemaßnahmen.

B.9.2 Schwachstellenbewertung

Zweck der Schwachstellenbewertung ist es, Schwachstellen zu ermitteln, die später bei Penetrationstests ausgenutzt werden könnten, indem grundlegende Abfragen zu den auf den betreffenden Systemen laufenden Diensten durchgeführt werden. Die Schwachstellenbewertung umfasst mindestens die folgenden Aktivitäten:

- a) Externe Schwachstellenbewertung – die Ziele sind die Netzwerkgeräte und Server, die für Dritte (sowohl Personen als auch Unternehmen) über eine öffentliche IP (öffentlich zugänglich) zugänglich sind und mit dem System in Verbindung stehen, von dem aus ein Zugriff auf personenbezogene Daten und andere sensible Informationen möglich ist.
- b) Interne Schwachstellenbewertung – die Ziele sind die intern zugänglichen Server (innerhalb der DMZ oder innerhalb des LAN, wenn es keine DMZ gibt), die mit dem System verbunden sind, von dem aus ein Zugriff auf personenbezogene Daten und andere sensible Informationen möglich ist. Jede Sicherheitsdomäne des internen Netzes ist gesondert zu testen.

B.9.3 Penetrationstests

Der Zweck der Penetrationstests besteht darin, alle Schwachstellen auszunutzen, die während der Schwachstellenbewertung in öffentlich zugänglichen Anwendungen oder Systemen aufgedeckt wurden, die Anwendungen enthalten, die personenbezogene Daten und andere sensible Informationen verarbeiten, übermitteln und/oder speichern. Die Penetrationstests umfassen mindestens die folgenden Aktivitäten:

- a) Penetrationstest auf der Netzwerkebene – der Test ahmt die Handlungen eines tatsächlichen Angreifers nach, der Schwachstellen in der Netzwerksicherheit ausnutzt und untersucht die Systeme auf Schwachstellen, die von einem externen Angreifer ausgenutzt werden könnten, um die Vertraulichkeit, Verfügbarkeit und/oder Integrität des Netzwerks zu beeinträchtigen.
- b) Penetrationstest auf der Anwendungsebene – bei diesem Test werden Tools eingesetzt, um Schwachstellen in den Anwendungen anhand von authentifizierten und nicht authentifizierten Scans zu identifizieren, die Ergebnisse zu analysieren, um falsch-positive Ergebnisse zu entfernen, und manuelle Tests durchzuführen, um die Ergebnisse der Tools zu bestätigen und die Auswirkungen der Schwachstellen zu ermitteln.

B.9.4 Überprüfung der Firewall-Regeln

Falls von der Regulierungsbehörde gefordert, sind die Firewall-Regeln regelmäßig zu überprüfen, um den Betriebszustand der Firewall und die Wirksamkeit ihrer Sicherheitskonfiguration und Regelsätze zu verifizieren; dies gilt für alle Perimeter-Firewalls und internen Firewalls.

: Betriebs-Audit für Dienstleistungsanbieter

C.1 Einleitung

C.1.1 Allgemeines

In diesem Anhang werden Verfahren und Praktiken für die Bewertung von Anbietern bestimmter Dienstleistungen dargelegt, die in einem Betriebs-Audit als Teil der Bewertung des interaktiven Glücksspielsystems überprüft werden, einschließlich, aber nicht beschränkt auf die Bewertung von Informationssicherheitsdiensten, Cloud-Diensten, Zahlungsdiensten (Finanzinstitute, Zahlungsabwickler usw.), Standortdiensten, Live-Spiel-Diensten und allen anderen Diensten, die direkt vom Betreiber angeboten werden oder die Inanspruchnahme von Drittanbietern beinhalten können.

HINWEIS: Es wird ebenfalls anerkannt, dass zusätzliche Verfahrensweisen und Praktiken, die nicht speziell in diese Norm eingeschlossen sind, für ein Betriebs-Audit relevant und erforderlich sind, wenn dies vom Betreiber und/oder der Regulierungsbehörde innerhalb ihrer Regeln, Vorschriften und internen Mindestkontrollstandards (MICS) bestimmt wurde.

C.2 Dienstleistungen zur Informationssicherheit

C.2.1 Audit des Informationssicherheits-Managementsystems (ISMS)

Der Betreiber oder ein dritter Anbieter von Informationssicherheitsdiensten, der Verwaltungs-, Unterstützungs-, Sicherheits- oder Notfallwiederherstellungsdienste für das System erbringt, muss sich einem speziellen, von der Regulierungsbehörde vorgeschriebenen, Audit unterziehen. Ihr Informationssicherheits-Managementsystem (ISMS) wird anhand der allgemeinen Grundsätze der Informationssicherheit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit überprüft, wie sie im Anhang zu „Betriebs-Audit für technische Sicherheitskontrollen“ und in diesem Abschnitt behandelt werden. Wenn die Regulierungsbehörde die Durchführung dieses Audits erlaubt, können die Ergebnisse früherer Audits genutzt werden, die von entsprechend akkreditierten Anbietern und qualifizierten Personen innerhalb des aktuellen Auditzeitraums (z. B. innerhalb des letzten Jahres) anhand von Normen wie ISO/IEC 27001, dem NIST Cybersecurity Framework (CSF) oder gleichwertigen Normen durchgeführt wurden. Eine solche Nutzung wird entsprechend im Prüfbericht vermerkt.

C.2.2 Informationssicherheitsrichtlinie

Es muss eine Informationssicherheitsrichtlinie in Kraft sein, die den Ansatz des ISMS für die Verwaltung der Informationssicherheit und dessen Umsetzung beschreibt. Die Informationssicherheitsrichtlinie muss:

- a) eine Bestimmung enthalten, die eine Überprüfung in geplanten Abständen und bei Änderungen des interaktiven Spielsystems oder der Verfahren des Betreibers, die das Risikoprofil des Systems verändern, vorschreibt;

- b) von der Geschäftsleitung genehmigt und allen Mitarbeitern des Betreibers und relevanten Mitarbeitern von Drittanbietern mitgeteilt werden; und
- c) die Sicherheitsrollen und Verantwortlichkeiten der Mitarbeiter des Betreibers und der relevanten Mitarbeiter von Drittanbietern für den Betrieb, die Wartung und die Instandhaltung des interaktiven Spielsystems und/oder seiner Komponenten festlegen;

C.2.3 Zugriffsrichtlinie

Im Rahmen des ISMS ist eine Zugriffsrichtlinie festzulegen und zu dokumentieren, die in regelmäßigen Abständen auf der Grundlage der Geschäfts- und Sicherheitsanforderungen für den physischen und logischen Zugang zum interaktiven Spielsystem und/oder seinen Komponenten zu überprüfen ist.

- a) Für die Gewährung und den Entzug des Zugriffs auf das interaktive Spielsystem und/oder seine Komponenten muss ein förmliches Verfahren zur Registrierung und Abmeldung von Benutzern vorhanden sein.
- b) Die Zuweisung von Zugriffsrechten wird auf der Grundlage der geschäftlichen Anforderungen und des Prinzips der geringsten Berechtigung eingeschränkt und kontrolliert.
- c) Die Mitarbeiter erhalten nur Zugang zu den Diensten oder Einrichtungen, zu deren Nutzung sie ausdrücklich ermächtigt wurden.
- d) Die Mitarbeiter erhalten angemessene Schulungen zum Sicherheitsbewusstsein und regelmäßige Aktualisierungen der organisatorischen Richtlinien und Verfahren, die für ihre Tätigkeit erforderlich sind.
- e) Die Geschäftsleitung muss die Zugriffsrechte der Benutzer in regelmäßigen Abständen anhand eines formalen Verfahrens überprüfen.
- f) Die Zugriffsrechte der Mitarbeiter auf das interaktive Spielsystem und/oder seine Komponenten werden bei Beendigung des Arbeitsverhältnisses, des Vertrags oder der Vereinbarung aufgehoben oder bei Änderungen angepasst.

C.2.4 Zuweisung von Sicherheitszuständigkeiten

Die Sicherheitszuständigkeiten müssen im Rahmen des ISMS wirksam dokumentiert und umgesetzt werden.

- a) Ein Sicherheitsforum, das sich aus Mitgliedern der Geschäftsleitung zusammensetzt, ist förmlich einzurichten, um das ISMS zu überwachen und zu überprüfen, um dessen fortdauernde Eignung, Angemessenheit und Wirksamkeit zu gewährleisten, sowie um förmliche Sitzungsprotokolle zu führen und in regelmäßigen Abständen, wie von der Regulierungsbehörde gefordert, zusammenzukommen.
- b) Es muss eine Sicherheitsabteilung vorhanden sein, die für die Entwicklung und Umsetzung von Sicherheitsstrategien und Aktionsplänen verantwortlich ist. Die Sicherheitsabteilung muss:
 - i. an allen Verfahren, die Sicherheitsaspekte des Betreibers betreffen, beteiligt sein und diese überprüfen, einschließlich, aber nicht beschränkt auf den Schutz von Informationen, Kommunikation, physischer Infrastruktur und Spielprozessen;
 - ii. keinen geringeren als der Geschäftsleitung unterstellt sein und nicht in der IT-Abteilung angesiedelt oder dieser unterstellt sein; und

- iii. über die erforderlichen Kompetenzen und Befugnisse verfügen und Zugang zu allen notwendigen Ressourcen haben, um eine angemessene Risikobewertung, -verwaltung und -reduzierung zu ermöglichen.
- c) Der Leiter der Sicherheitsabteilung muss Mitglied des Sicherheitsforums sein und ist für die Empfehlung von Sicherheitsrichtlinien und -änderungen verantwortlich.

C.2.5 Störfallmanagement

Ein Verfahren für die Meldung von Informationssicherheitsvorfällen und die entsprechende Reaktion der Geschäftsleitung ist im Rahmen des ISMS gemäß der Informationssicherheitsrichtlinie zu dokumentieren und umzusetzen. Das Verfahren für das Störfallmanagement muss:

- a) eine Definition dessen umfassen, was einen Informationssicherheitsvorfall darstellt;
- b) dokumentieren, wie Informationssicherheitsvorfälle über angemessene Kanäle zur Geschäftsleitung gemeldet werden;
- c) Zuständigkeiten und Verfahren der Geschäftsleitung zur Gewährleistung einer schnellen, wirksamen und ordnungsgemäßen Reaktion auf Informationssicherheitsvorfälle enthalten, einschließlich:
 - i. Verfahren für den Umgang mit verschiedenen Arten von Informationssicherheitsvorfällen;
 - ii. Verfahren für die Analyse und Identifizierung der Ursache des Vorfalls;
 - iii. Kommunikation mit den von dem Vorfall betroffenen Personen;
 - iv. Meldung des Vorfalls an die zuständige Behörde;
 - v. Sammlung forensischer Beweise; und
 - vi. eine kontrollierte Wiederherstellung nach Informationssicherheitsvorfällen.

C.3 Cloud-Dienste

C.3.1 Audit von Cloud-Diensteanbietern

Ein Betreiber, der einen von der Regulierungsbehörde zugelassenen Cloud-Diensteanbieter für die Speicherung, Übertragung oder Verarbeitung von personenbezogenen Daten und anderen sensiblen Informationen in Anspruch nimmt, muss sich einer von der Regulierungsbehörde geforderten spezifischen Prüfung unterziehen. Der Betrieb des Cloud-Diensteanbieters wird anhand der allgemeinen Grundsätze der Informationssicherheit in Bezug auf die Bereitstellung und Nutzung von Cloud-Diensten überprüft, die im Anhang zu „Betriebs-Audit für technische Sicherheitskontrollen“ und in diesem Abschnitt behandelt werden. Wenn die Regulierungsbehörde die Durchführung dieses Audits erlaubt, können die Ergebnisse früherer Audits genutzt werden, die von entsprechend akkreditierten Anbietern und qualifizierten Personen innerhalb des aktuellen Auditzeitraums (z. B. innerhalb des letzten Jahres) anhand von Normen wie ISO/IEC 27017 and ISO/IEC 27018 oder gleichwertigen Normen durchgeführt wurden. Eine solche Nutzung wird entsprechend im Prüfbericht vermerkt.

C.3.2 Beziehung zu Cloud-Dienstleistern

Die Sicherheit der Cloud liegt in der gemeinsamen Verantwortung des Cloud-Diensteanbieters und des Betreibers.

- a) Wenn personenbezogene Daten und andere sensible Informationen in einer Cloud-Umgebung gespeichert, verarbeitet oder übertragen werden, gelten die entsprechenden Anforderungen für diese Umgebung und beinhalten in der Regel eine Validierung sowohl der Infrastruktur des Cloud-Anbieters als auch der Nutzung dieser Umgebung durch den Betreiber.
- b) Die Aufteilung der Verantwortung für die Verwaltung der Sicherheitskontrollen zwischen dem Cloud-Diensteanbieter und dem Betreiber entbindet den Betreiber nicht von der Verantwortung, zu gewährleisten, dass personenbezogene Daten und andere sensible Informationen gemäß den geltenden Anforderungen ordnungsgemäß gesichert werden.
- c) Zwischen dem Cloud-Diensteanbieter und dem Betreiber sind klare Strategien und Verfahren für alle Sicherheitsanforderungen zu vereinbaren, und die Zuständigkeiten für Betrieb, Verwaltung und Berichterstattung müssen für jede anwendbare Anforderung klar definiert und nachvollziehbar sein.

C.4 Zahlungsdienste

C.4.1 Audit von Zahlungsdienstleistern

Der Betreiber oder ein dritter Zahlungsdienstleister, der für die Abwicklung von Transaktionen mit Finanzinstituten eingesetzt wird, muss sich einem spezifischen Audit unterziehen, das jeweils von der Regulierungsbehörde vorgeschrieben wird. Der Betrieb des Zahlungsdienstleisters wird anhand der allgemeinen Grundsätze der Informationssicherheit in Bezug auf die Bereitstellung und Nutzung von Zahlungsdienstleistern überprüft, die im Anhang zu „Betriebs-Audit für technische Sicherheitskontrollen“ und in diesem Abschnitt behandelt werden. Wenn die Regulierungsbehörde die Durchführung dieses Audits erlaubt, können die Ergebnisse früherer Audits genutzt werden, die von entsprechend akkreditierten Anbietern und qualifizierten Personen innerhalb des aktuellen Auditzeitraums (z. B. innerhalb des letzten Jahres) anhand von Normen wie die Payment Card Industry Data Security Standards (PCI-DSS) oder gleichwertigen Normen durchgeführt wurden. Eine solche Nutzung wird entsprechend im Prüfbericht vermerkt.

C.4.2 Gewährleistung der Zahlungssicherheit

Der Zahlungsdienstleister muss die im System verwendeten Zahlungsarten vor missbräuchlicher Nutzung schützen.

- a) Die Erhebung von personenbezogenen Daten und anderen sensiblen Informationen, die unmittelbar mit Finanztransaktionen zusammenhängen, ist auf die für die Transaktion unbedingt erforderlichen Informationen zu beschränken.
- b) Es müssen Verfahren vorhanden sein, anhand derer überprüft werden kann, ob der Zahlungsdienstleister die mit jeder Finanztransaktion unmittelbar verbundenen personenbezogenen Daten oder anderen sensiblen Informationen schützt.
- c) Alle Kommunikationskanäle zwischen dem Betreiber und dem Zahlungsdienstleister, über die Zahlungsdaten übermittelt werden, sind zu verschlüsseln und gegen Abhören zu schützen.
- d) Alle Finanztransaktionen werden täglich oder nach Maßgabe der Regulierungsbehörde zwischen dem Betreiber und dem Zahlungsdienstleister abgeglichen. Es müssen Verfahren festgelegt werden für:

- i. Bei der Berechnung der an einen Spieler gezahlten oder von ihm erhaltenen Beträge werden alle vom Spieler oder Betreiber verwendeten Zahlungen berücksichtigt; und
- ii. es wird sichergestellt, dass die Eigentumsverhältnisse zwischen dem Inhaber der Zahlungsart und dem Inhaber des Spielerkontos übereinstimmen.

C.5 Standortdienste

C.5.1 Audit von Standortdienstleistern

Der Betreiber oder ein dritter Anbieter von Standortdiensten, der Informationen zur Identifizierung und zum geografischen Standort von Spielern gemäß der Zulassung der Regulierungsbehörde bereitstellt, unterzieht sich einem von der Regulierungsbehörde geforderten spezifischen Audit, um seine kontinuierliche Fähigkeit zu bewerten und zu messen, bestehende und neu entstehende Risiken des Standortbetrugs zu erkennen und zu mindern, einschließlich der in diesem Abschnitt enthaltenen Kontrollen.

C.5.2 Standortdienste – Berichte und Analysen

Da Standortbetrug sowohl bei einer einzelnen Standortüberprüfung als auch bei kumulativen Spielerstandorten im Laufe der Zeit zu bewerten ist, muss der Anbieter von Standortdiensten:

- a) über Verfahren verfügen, die eine Echtzeit-Dateneinspeisung aller Standortüberprüfungen und eine aktuelle Liste potenzieller Standortbetrugsrisiken (z. B. gefälschte Standortanwendungen, virtuelle Maschinen, Remote-Desktop-Programme usw.) gewährleisten;
- b) über ein Warnsystem verfügen, um unbefugten oder unzulässigen Zugriff zu erkennen; und
- c) die routinemäßige, wiederkehrende Übermittlung zusätzlicher Betrugsberichte über verdächtige oder ungewöhnliche Aktivitäten, die gemeinsame Nutzung von Konten, Spielteilnehmer mit böswärtigen Absichten und Geräte sowie andere risikoreiche Transaktionsdaten ermöglichen.

C.5.3 Verwaltung der Standortdienste

Um die Gesamtintegrität des Standortdienstes aufrechtzuerhalten, muss der Anbieter des Standortdienstes die Standortermittlung oder die für die Standortermittlung verwendete Anwendung sicherstellen:

- a) Einsatz geschlossener Datenbanken (IP, Proxy, VPN usw.), die häufig aktualisiert und regelmäßig auf Genauigkeit und Zuverlässigkeit geprüft werden, und
- b) Durchführung regelmäßiger Updates, um die Datenerfassung, die Gerätekompatibilität und die Betrugsvorbeugungsfunktionen auf dem neuesten Stand zu halten und Betrugsrisiken bei der Standortbestimmung zu vermeiden.

C.6 Live-Spiel-Dienste

C.6.1 Audit von Anbietern von Live-Spielen

Der Anbieter von Live-Spielen muss die anwendbaren Aspekte der entsprechenden Richtlinien und/oder Verfahrensdokumente erfüllen, die vom Betreiber in Absprache mit der Regulierungsbehörde festgelegt wurden, einschließlich der in diesem Abschnitt enthaltenen Kontrollen. Um die Integrität des Verfahrens zur Ermittlung des Spielergebnisses zu wahren, können die Live-Spiel-Dienste je nach Anforderung der Regulierungsbehörde einem zusätzlichen Audit unterzogen werden.

C.6.2 Sicherheit in der Live-Spiel-Umgebung

Die Live-Spiel-Umgebung muss definiert sein und über angemessene physische Sicherheitskontrollen verfügen. Sichere Bereiche, Verbrauchsmaterialien und Geräte für Live-Spiele sind anhand geeigneter Zugangskontrollen und Sicherheitsverfahren zu schützen, um zu gewährleisten, dass nur befugten Mitarbeitern nach Maßgabe der folgenden Leitlinien der Zugang gestattet ist:

- a) Finden die Live-Spiele in einem Spiellokal (z. B. Casino, Bingohalle, Kartenspielraum usw.) statt, in dem der Spielbereich gemäß den Gesetzen und Normen der Regulierungsbehörde für das Spielen durch persönlich teilnehmende Spieler freigegeben ist, muss die Live-Spiel-Umgebung anhand derselben Regeln und Kontrollen wie das Spiellokal kontrolliert werden, einschließlich, aber nicht beschränkt auf:
 - i. die Sicherheitssysteme der Bereiche, in denen die Live-Spiele stattfinden; und
 - ii. die Kontrollen der Zugänge zu diesen Bereichen, um sicherzustellen, dass nur befugte Mitarbeiter diese betreten können, und die Kontrollen des gesamten Bereichs rund um die Geräte für Live-Spiele, um die Richtigkeit der Spielteilnehmer zu gewährleisten.
- b) Falls die Live-Spiele während der öffentlichen Öffnungszeiten in einem Spiellokal stattfinden und in einem Spielbereich, der nicht für das Spielen durch persönlich teilnehmende Spieler freigegeben ist:
 - i. Die Bereiche, in denen die Live-Spiele stattfinden, sowie der gesamte Bereich rund um die Geräte für Live-Spiele und die dazugehörigen Zugänge müssen mindestens durch Abgrenzungen und Warnschranken abgegrenzt und durch Sicherheitspersonal überwacht werden; und
 - ii. die Geräte für Live-Spiele unterliegen denselben Zugangskontrollen, als ob sie sich in einem Spiellokal befänden.
- c) Falls die Live-Spiele in einem privaten Spiellokal oder in einem Spiellokal außerhalb der Öffnungszeiten für die Öffentlichkeit oder in einem Spielbereich stattfinden, der nicht für persönliche teilnehmende Spieler geöffnet ist und nicht durch das Sicherheitspersonal überwacht wird:
 - i. Die Bereiche, in denen die Live-Spiele stattfinden, sowie der gesamte Bereich rund um die Geräte für Live-Spiele und die dazugehörigen Zugänge sind durch physische Barrieren abzusperren und die entsprechenden Zugänge durch Zugangssicherheitssysteme zu sichern; und
 - ii. Zugangspunkte wie Liefer- und Ladebereiche und andere Punkte, an denen Unbefugte die Bereiche, in denen die Live-Spiele stattfinden, betreten können, sind zu kontrollieren und nach Möglichkeit von den Betriebsbereichen abzutrennen, um unbefugten Zugang zu verhindern.

C.6.3 Überwachung und Aufzeichnung

Der Anbieter von Live-Spielen ist verpflichtet, ein Überwachungssystem zu installieren, zu warten und zu betreiben, das in der Lage ist, ununterbrochene und ungehinderte Sicht auf alle Live-Spiele zu überwachen und aufzuzeichnen.

- a) Alle gespielten Spiele müssen kontinuierlich aufgezeichnet werden, damit:
 - i. Die Informationen, die erforderlich sind, um jedes Spiel in Übereinstimmung mit den geltenden Rückrufanforderungen im Abschnitt „Erforderliche Informationen zum letzten Spiel“ angemessen zu rekonstruieren, die nicht von der Spielplattform selbst angezeigt werden, identifizierbar und unterscheidbar sind;
 - ii. Datum und Uhrzeit jedes Spiels mit einer Genauigkeit von einer Sekunde relativ zu der vom System verwendeten Uhr bestimmt werden können; und
 - iii. die Reihenfolge der Spiele zueinander bestimmt werden kann.
- b) Es müssen Verfahren vorhanden sein, die gewährleisten, dass die Aufzeichnung:
 - i. die definierte Live-Spiel-Umgebung mit ausreichender Detailgenauigkeit abdeckt, um zu bestätigen, ob die Spielregeln und -verfahren eingehalten wurden, und um Unstimmigkeiten zu identifizieren;
 - ii. so aufgezeichnet wird, dass eine Beeinflussung oder Löschung ausgeschlossen ist;
 - iii. vom Betreiber und/oder der Regulierungsbehörde im Falle einer Spielerbeschwerde/eines Rechtsstreits überprüft werden kann; und
 - iv. mindestens neunzig Tage lang oder für den von der Regulierungsbehörde geforderten Zeitraum aufbewahrt wird.

C.6.4 Simulcast-Kontrollserver

Der Anbieter von Live-Spielen verwendet Simulcast-Kontrollserver für die Aufzeichnung aller Spielaktivitäten und Ergebnisse. Der Anbieter von Live-Spielen kann seine eigene Überwachungskamera verwenden und die Live-Übertragung auf den Simulcast-Kontrollserver aufteilen, oder es kann ein separates Videonetzwerk verwendet werden. Die Simulcast-Kontrollserver müssen:

- a) dem Spieler einen audiovisuellen Echtzeit-Zugang zum laufenden Spiel bieten, einschließlich:
 - i. aller Informationen, die in den Abschnitten „Spielinformationen und Spielregeln“ und „Anzuzeigende Informationen“ zu finden sind und nicht von der Spielplattform selbst angezeigt werden;
 - ii. der Handlungen des Spielleiters und gegebenenfalls anderer Spielteilnehmer;
 - iii. Datum und Uhrzeit am Spiellokal; und
 - iv. Spielidentifikation/Tischnummer sowie Standort.
- b) Jedem Spielteilnehmer wird eine Video-/Audioübertragung in gleichwertiger Qualität zur Verfügung gestellt.
 - i. Diese Gleichwertigkeit ist zu messen und zu überprüfen, sobald eine Kommunikation eingeleitet wird, einschließlich der Wiederherstellung der Verbindung bei Signalunterbrechungen oder der Wiedereinleitung, wenn das Signal unterbrochen wurde.
 - ii. Es ist eine Mindestanforderung für die Signalverbindung festzulegen, durchzusetzen und den Spielern mitzuteilen.

- c) Es muss verhindert werden, dass jemand auf das Live-Spielergebnis zugreifen kann, bevor eine Wette abgeschlossen wurde.
- d) Spielergebnisse müssen vor der Veröffentlichung auf der Spieleplattform aufgezeichnet werden.
- e) Es muss ein Mechanismus zur Verfügung stehen, der es einem autorisierten Mitarbeiter ermöglicht, Spielergebnisse zu stornieren, falls dies erforderlich ist.

C.6.5 Geräte für Live-Spiele

Der Anbieter von Live-Spielen stellt einen sicheren Ort für die Aufstellung, den Betrieb und die Nutzung von Geräten für Live-Spiele, einschließlich Simulcast-Kontrollservern, Spielservern und Kommunikationsausrüstung, zur Verfügung. Es müssen Sicherheitsrichtlinien und -verfahren vorhanden sein, die regelmäßig überprüft werden, um zu gewährleisten, dass Risiken erkannt, gemindert und durch Notfallpläne abgesichert werden. Darüber hinaus müssen die Geräte für Live-Spiele den von der Regulierungsbehörde festgelegten Mindeststandards sowie den folgenden Anforderungen entsprechen:

- a) Geräte für Live-Spiele müssen nach einem festgelegten Plan aufgestellt werden, und es müssen Aufzeichnungen über alle aufgestellten Geräte geführt werden.
- b) Geräte für Live-Spiele müssen so aufgestellt oder geschützt werden, dass die Risiken durch folgende Faktoren verringert werden:
 - i. Umweltbedrohungen und -gefahren;
 - ii. Gelegenheiten für unbefugten Zugriff;
 - iii. Stromausfälle; und
 - iv. andere Störungen, die durch Ausfälle der Versorgungseinrichtungen verursacht werden.
- c) Der Zugang des Spielleiters zum Gerät für Live-Spiele wird durch ein sicheres Anmeldeverfahren oder ein anderes sicheres, von der Regulierungsbehörde zugelassenes Verfahren kontrolliert, um sicherzustellen, dass nur autorisierte Spielleiter Zugang erhalten. Es darf nicht möglich sein, die Konfigurationseinstellungen des Geräts für Live-Spiele ohne ein autorisiertes sicheres Verfahren zu ändern.
- d) Eine Benutzersitzung wird, sofern sie von einem Gerät für Live-Spiele unterstützt wird, dadurch eingeleitet, dass sich der Spielteilnehmer in sein Benutzerkonto einloggt, indem er seinen sicheren Benutzernamen und sein Passwort oder ein anderes, von der Regulierungsbehörde zugelassenes Mittel zur Identifizierung des Spielteilnehmers verwendet.
 - i. Alle verfügbaren Optionen, die dem Spielteilnehmer angeboten werden, sind an sein Benutzerkonto gebunden.
 - ii. Wenn das Gerät für Live-Spiele innerhalb von fünf Minuten oder einer von der Regulierungsbehörde festgelegten Zeitspanne keine Eingaben des Spielteilnehmers erhält, wird die Benutzersitzung unterbrochen oder gesperrt, so dass sich der Spielteilnehmer erneut anmelden muss, um fortzufahren.
- e) Um die ständige Verfügbarkeit und Integrität des Geräts für Live-Spiele zu gewährleisten, muss es in regelmäßigen Abständen von ausgewiesenem Personal ordnungsgemäß gewartet und inspiziert werden, um sicherzustellen, dass es frei von Defekten oder Mechanismen ist, die seinen Betrieb beeinträchtigen könnten.
- f) Vor der Entsorgung oder Wiederverwendung sind Geräte für Live-Spiele mit Speichermedien zu überprüfen, um zu gewährleisten, dass lizenzierte Software und andere sensible Informationen entfernt oder sicher überschrieben (d. h. nicht nur gelöscht) wurden.

C.6.6 Verbrauchsmaterialien für Live-Spiele

Die von Live-Spiel-Diensten verwendeten Verbrauchsmaterialien müssen den von der Regulierungsbehörde festgelegten Mindeststandards sowie den folgenden Anforderungen entsprechen:

- a) Es sind Verfahren einzuführen, anhand derer der Bestand an Verbrauchsmaterial von der Entgegennahme über die Lagerung, Installation, Verwendung, Ausmusterung und Vernichtung verfolgt werden kann. Alle Verbrauchsmaterialien müssen mit einem Prüfpfad versehen sein, aus dem hervorgeht, welches benannte Personal zu einem bestimmten Zeitpunkt und für einen bestimmten Vorgang Zugang zu den Verbrauchsmaterialien hatte;
- b) es müssen regelmäßige Stichprobenkontrollen der verwendeten Verbrauchsmaterialien von der Auszahlung bis zur Ausmusterung erfolgen; und
- c) benutztes Verbrauchsmaterial ist so zu vernichten, dass eine versehentliche Wiederverwendung bei Live-Spielen verhindert und das Verbrauchsmaterial dauerhaft unbrauchbar wird.

C.6.7 Physische Spielerchips

Die folgenden Kontrollen gelten für physische Spielerchips, die in Live-Spielen verwendet werden. Bei einem Live-Pokerspiel, an dem sowohl persönlich teilnehmende Spieler als auch Spieler beteiligt sind, die über eine Spielplattform spielen, können beispielsweise physische Spielerchips auf dem Tisch platziert werden, um den anderen Spielern den Einsatz des Spielers anzuzeigen.

- a) Alle Chips müssen die gleichen physischen Merkmale aufweisen, abgesehen von spezifischen Unterschieden in der Stückelung.
- b) Es müssen die Chips aller möglichen Stückelungen angezeigt werden (entsprechend der Stückelung im Spiel), so dass die Nichtverfügbarkeit von Chips mit kleineren Stückelungen die Spieler nicht dazu zwingt, mehr zu setzen.
- c) Jeder Chip muss so gestaltet sein, dass dessen spezifische Stückelung bestimmt werden kann, wenn er sich in einem Stapel von Chips mit verschiedenen Stückelungen befindet.
- d) Die verwendeten Chips müssen für jede Stückelung, die sie jeweils darstellen, einzigartig sein, und die Stückelung muss auf jedem Chip deutlich sichtbar sein.

C.6.8 Verfahren für Live-Spiele

Die folgenden Verfahren müssen für Anbieter von Live-Spielen vorhanden sein. Diese Verfahren sind regelmäßig zu überprüfen, um sicherzustellen, dass Risiken erkannt, gemindert und durch Notfallpläne abgesichert werden.

- a) Es müssen Verfahren vorhanden sein, die eine angemessene Reaktion auf jedes Sicherheitsproblem innerhalb der Live-Spiel-Dienste ermöglichen.
- b) Es müssen Verfahren vorhanden sein, die verhindern, dass jemand den Betrieb von Live-Spielen oder Geräte für Live-Spiele manipuliert oder beeinträchtigt.
- c) Für jedes Spiel gibt es gesonderte Verfahren, und für neue Spiele müssen diese Verfahren vorhanden sein, bevor sie den Spielteilnehmern angeboten werden.

- d) Für das Personal des Anbieters von Live-Spielen, einschließlich der Spielbetreuer, müssen die folgenden, von der Regulierungsbehörde vorgeschriebenen Verfahren vorhanden sein:
- i. Es müssen Verfahren zur regelmäßigen Hintergrundüberprüfung des Personals vorhanden sein;
 - ii. das Personal muss angemessen geschult sein, um Live-Spiele auf faire Weise gemäß den dokumentierten Verfahren und Spielregeln anbieten zu können. Nachweise über die Schulung und regelmäßige Auffrischungsschulungen sind aufzubewahren;
 - iii. das Personal ist zu schulen und regelmäßig daran zu erinnern, welche körperlichen Verhaltensweisen verboten oder vorgeschrieben sind (einschließlich Handzeichen, Sprechen, Umgang mit Karten usw.);
 - iv. Richtlinien und Verfahren für Rotationen, Schichtmuster und Zuteilung sind zu dokumentieren, einschließlich der Zuteilung von Spielbetreuern zu Tischen/Spielen (d. h. ohne vorherige Kenntnis der Tische/Spiele, die sie bedienen werden, und mit einer Zeit, die entsprechend festgelegt ist, so dass keine schädlichen Beziehungen entstehen) sowie Änderungen bei den Spielbetreuern unter außergewöhnlichen Umständen;
 - v. eine Methode zur angemessenen Erkennung von Spielern, die Tische/Spiele ablehnen und daraufhin Tischen/Spielen innerhalb derselben Spielart beitreten möchten, bis sie ihren bevorzugten Tisch/ihr bevorzugtes Spiel erreichen;
 - vi. die Aufbewahrung von Unterlagen muss solide sein, damit die Aufzeichnungen des Personals geprüft und Untersuchungen durchgeführt werden können, wenn Mitarbeiter entweder direkt beteiligt sind oder wenn ihre Anwesenheit an einem bestimmten Ort und/oder zu einer bestimmten Zeit für das Verständnis einer Ereigniskette entscheidend ist;
 - vii. die Verfahren für die Einstellung und Entlassung von Mitarbeitern sind zu dokumentieren;
 - viii. bei Live-Spielen muss immer eine Aufsichtsperson anwesend sein;
 - ix. für jeden Tisch/jedes Spiel sind Personalprotokolle zu führen; und
- e) es müssen Verfahren vorhanden sein, um die persönlich teilnehmenden Spieler darüber in Kenntnis zu setzen, dass sie als Teil einer Live-Übertragung gefilmt werden.
- f) Verfahren in Bezug auf ungewöhnliche Ereignisse, die während Live-Spielen auftreten können, müssen dokumentiert und vom Personal verstanden werden, einschließlich, aber nicht beschränkt auf:
- i. Fehlfunktionen von Spezialgeräten oder physischen Zufallsgeräten, einschließlich der Erkennung falscher Ergebnisse;
 - ii. Fallengelassene Karten;
 - iii. Falsch ausgegebene Karten;
 - iv. Neudreh;
 - v. Abgebrochene Spiele; und
 - vi. und Schließungen von Tischen/Spielen.
- g) Es müssen einheitliche Verfahren für das Mischen der Karten vorhanden sein, einschließlich einer Überprüfung der Kartenanzahl, der Häufigkeit des Mischens und der Fälle, in denen die Karten neu gemischt werden. Das Mischen der Karten ist zu protokollieren.
- h) Es muss ein festgelegtes Verfahren für die Abrechnung der physischen Spielerchips bestehen.
- i) Es müssen Verfahren vorhanden sein, mit denen nachgewiesen wird, dass ein einzelner Mitarbeiter nicht in der Lage ist, alle Aufgaben im Zusammenhang mit der Spielleitung zu übernehmen, und dass eine Trennung der Zuständigkeiten vor, während und nach dem Spiel besteht.

- j) Es müssen Verfahren für den Fall vorhanden sein, dass die Verbindung zu den Spielteilnehmern oder die Video-, Sprach- oder Datenübertragung während eines Live-Spiels unterbrochen wird.
- k) Es müssen Verfahren vorhanden sein, die gewährleisten, dass für Einsätze bei Live-Spielen:
 - i. wenn Einsätze durch mündliche Anweisungen getätigt werden, der Inhalt des Wetteinsatzes dem Spieler durch Wiederholung bestätigt wird, bevor der Wetteinsatz bestätigt wird;
 - ii. wenn ein Spielbetreuer die vom Spieler angegebenen Einsätze entgegennimmt, der Spielteilnehmer einen eindeutigen Hinweis oder eine Mitteilung erhält, ob der Einsatz (ganz oder teilweise) angenommen oder abgelehnt wurde; und
 - iii. der Spielteilnehmer mit Gewinn nach Beendigung des Spiels über seinen Gewinn, einschließlich des gewonnenen Betrags, benachrichtigt wird und dass sein Kontostand entweder sofort oder nach Verlassen des Spiels aktualisiert wird.
- l) Variationen in der Funktionsweise von Kartenmischern und -schlitten, Roulettekesseln, Kugelgebläsen, Würfelbechern oder anderen Geräten für Live-Spiele müssen in die Spielabläufe integriert werden, um die Zufälligkeit zu erhalten. Diese Geräte müssen ein Zufallsniveau aufweisen, das dem in Spiellokalen üblichen entspricht, um ihre Fairness und Integrität zu gewährleisten.
- m) Es müssen Verfahren vorhanden sein, die gewährleisten, dass Kartenschlitten und ähnliche Spezialgeräte sowie physische Zufallsgeräte nach dem Laden manipulationssicher sind, um Störungen vor und während des Spiels auszuschließen.
- n) Um ihre Integrität zu gewährleisten und aufrechtzuerhalten, müssen alle Spezialgeräte und physischen Zufallsgeräte regelmäßig inspiziert und auf ihre Zuverlässigkeit getestet werden. Darüber hinaus:
 - i. Alle Verbrauchsmaterialien oder Geräte für Live-Spiele, die mit dieser Hardware in Berührung kommen, müssen vor der Verarbeitung auf Defekte überprüft werden, um Spielunterbrechungen zu vermeiden; und
 - ii. über alle Tests sind Protokolle zu führen.
- o) Es müssen Verfahren vorhanden sein, die den Spieler informieren, wenn der manuelle Betriebsmodus des Spezialgeräts aktiviert ist, und die Verfolgung muss aktiviert sein, um eine weitere Überprüfung zu ermöglichen.
- p) Es müssen Richtlinien und Verfahren vorhanden sein, um Spezialgeräte und physische Zufallsgeräte zu identifizieren und zu ersetzen, die eine inakzeptable Fehlerquote aufweisen.
- q) Es müssen Verfahren vorhanden sein, um Spielprotokolle zu führen und Spielereignisse in Statistiken zusammenzufassen, die auf Trends in Bezug auf die Spielleistung, das Personal und/oder die Standorte in der Live-Spielumgebung analysiert werden können, einschließlich derjenigen für Aufsichtspersonen, Schichten, Verfahrensverstöße sowie andere Vorfälle, Unregelmäßigkeiten und Fehler.

Glossar der wichtigsten Begriffe

Zugangskontrolle – der Prozess der Gewährung oder Verweigerung spezifischer Anfragen für den Erhalt und die Nutzung sensibler Informationen und zugehöriger Dienste, die spezifisch für ein System sind, und für den Zugang zu bestimmten physischen Einrichtungen, in denen sich kritische Netz- oder Systeminfrastrukturen befinden.

Angegebene Prämie – eine Prämie, die in einem Spiel vergeben werden kann und die dem Spieler in der Spielgrafik ausdrücklich angekündigt wird.

Algorithmus – eine endliche Menge eindeutiger Anweisungen, die in einer vorgeschriebenen Reihenfolge ausgeführt werden, um ein Ziel zu erreichen, insbesondere eine mathematische Regel oder ein Verfahren, das zur Berechnung eines gewünschten Ergebnisses verwendet wird. Algorithmen sind die Grundlage für die meisten Computerprogramme.

Alternativer Spielmodus – jeder Spielmodus, der vom normalen Spielmodus abweicht. Dazu gehören Modi wie Automatischer Spielmodus, Turnier und Freispielmodus.

ARP, Address Resolution Protocol – das Protokoll, das zur Übersetzung von IP-Adressen in MAC-Adressen verwendet wird, um die Kommunikation in einem drahtlosen oder verdrahteten lokalen Netzwerk zu ermöglichen.

Illustrationen – die Grafiken, thematischen Grafiken, Hilfebildschirme und andere Textinformationen, die dem Spieler auf der Benutzeroberfläche angezeigt werden.

Prüfpfad – eine Aufzeichnung, die zeigt, wer auf ein System zugegriffen hat und welche Aktionen der Benutzer während eines bestimmten Zeitraums durchgeführt hat.

Authentifizierung – Überprüfung der Identität eines Benutzers, eines Prozesses, eines Softwarepakets oder eines Geräts, oft als Voraussetzung für den Zugriff auf Ressourcen in einem System.

Automatisierte Entscheidungsfindung – die Fähigkeit, mit technischen Mitteln Entscheidungen auf der Grundlage von personenbezogenen Daten oder direkt bereitgestellten Daten zu treffen. Damit eine Art der Verarbeitung als automatisiert und nicht als ausschließlich automatisiert eingestuft werden kann, muss eine sinnvolle menschliche Beteiligung an dem Prozess vorhanden sein (z. B. durch Überprüfung oder Filterung), und diese menschliche Beteiligung muss vor der endgültigen Entscheidung erfolgen.

Automatischer Spielmodus – ein vom Spieler wählbarer Modus eines Spiels, der es dem Spieler ermöglicht, Einsätze automatisch und ohne manuelle Interaktion zu platzieren, sobald eine Stückelung, ein Einsatz und andere Spieleigenschaften für das Spiel ausgewählt wurden.

Datensicherung (Backup) – eine Kopie von Dateien und Programmen, die erstellt wird, um die Wiederherstellung im Bedarfsfall zu erleichtern.

Best-Hand-Spiel – eine Methode der geheimen Absprache, bei der zwischen zwei oder mehr Spielern immer nur derjenige spielt, der das beste Ergebnis hat, während der andere oder die anderen das Spiel verlassen.

Biometrik – eine biologische Identifikationseingabe, wie z. B. Fingerabdrücke oder Netzhautmuster.

Bonusprämie – eine Anreizprämie, die auf einem Spielereignis oder einem externen Auslöser basiert und keine Auslöser umfasst, die auf einer bestimmten Aktivität des Spielerkontos basieren. Beispiele hierfür sind Multiplikationsprämien, bei denen das Spiel alle Gewinne innerhalb eines bestimmten Bereichs mit einem bestimmten Wert multipliziert, oder eine Münze, die gewonnen wird, wenn ein Prozentsatz des Spiels bei teilnehmenden Spielen einen zufällig ausgewählten Wert erreicht.

Cache Poisoning – ein Angriff, bei dem der Angreifer beschädigte Daten in die Cache-Datenbank des Domain Name Service (DNS) einfügt.

Chip Dumping – eine Absprache, bei der sich zwei oder mehr Spieler gegenseitig helfen, im Spiel zu bleiben, d. h. Spielteilnehmer verlieren bei einer Hand mit einer sicheren Gewinnkombination absichtlich, um auf diese Weise einem anderen Spieler Chips zu überlassen.

Kommunikationstechnologie – jedes Verfahren und jede Komponente, die zur Erleichterung der Übertragung und des Empfangs von Informationen eingesetzt wird, einschließlich der Übertragung und des Empfangs durch Systeme, die drahtgebundene, drahtlose, WLAN-, Funk-, Mikrowellen-, Licht-, Glasfaser-, Satelliten- oder Computerdatennetze, einschließlich Internet und Intranets, verwenden.

Gemeinschaftsbonus – eine Art von Bonus/Bonusspiel, bei dem die Spieler zusammenarbeiten und/oder um einen gemeinsamen Preis kämpfen.

Beiträge – die finanzielle Methode, mit der die Pools für progressive Jackpots oder stufenweise Jackpots finanziert werden.

Notfallplan – Verwaltungsrichtlinie und -verfahren zur Aufrechterhaltung oder Wiederherstellung des Spielbetriebs im Falle von Notfällen, Systemausfällen oder Katastrophen, wobei dies möglicherweise an einem alternativen Standort erfolgen kann.

Guthabenanzeige – eine Anzeige, die das dem Spieler zur Verfügung stehende Guthaben für den Einsatz hält, der auf das Spielerkonto und von diesem übertragen wird.

Kritische Komponente – jedes Teilsystem, dessen Ausfall oder Kompromittierung zum Verlust von Spieleransprüchen, staatlichen Einnahmen oder unbefugtem Zugriff auf Daten führen kann, die zur Erstellung von Berichten für die Regulierungsbehörde verwendet werden. Beispiele für kritische Komponenten sind: Komponenten, die personenbezogene Daten und andere sensible Informationen aufzeichnen, speichern, verarbeiten, weitergeben, übermitteln oder abrufen (z. B. Validierungsnummern, Authentifizierungsnachweise usw.); Komponenten, die Zufallszahlen zur

Ermittlung des Spielergebnisses erzeugen, übermitteln oder verarbeiten; Komponenten, die die Ergebnisse des aktuellen Stands des Einsatzes eines Spielteilnehmers speichern; Zugangs- und Ausgangspunkte zu den oben genannten Komponenten (andere Systeme, die direkt mit kritischen Kernsystemen kommunizieren); und Kommunikationsnetze, die personenbezogene Daten und andere sensible Informationen übertragen.

Kritisches Kontrollprogramm – ein Softwareprogramm, das das Verhalten in Bezug auf geltende technische Normen und/oder gesetzliche Vorschriften kontrolliert.

Kryptographischer RNG – ein Zufallszahlengenerator (Random Number Generator, RNG), der gegen einen Angriff oder eine Kompromittierung durch einen intelligenten Angreifer mit modernen Rechenressourcen, der den Quellcode des Zufallszahlengenerator und/oder seinen Algorithmus kennt, resistent ist. Kryptografische RNGs können nicht kompromittiert werden, um zukünftige Werte vorherzusagen.

Datenintegrität – die Eigenschaft, dass Daten sowohl richtig als auch konsistent sind und weder bei der Speicherung noch bei der Verarbeitung oder bei der Übertragung auf unbefugte Weise verändert wurden.

DDOS, *Distributed Denial of Service* – eine Angriffsart, bei der mehrere kompromittierte Systeme, die in der Regel mit einem destruktiven Softwareprogramm infiziert sind, verwendet werden, um ein einzelnes System anzugreifen. Zu den Opfern eines DDOS-Angriffs gehören sowohl das Zielsystem als auch alle Systeme, die der Hacker bei dem verteilten Angriff böswillig verwendet und kontrolliert.

Zahlungsinstrument – eine Karte, ein Code oder ein anderes Gerät, mit dem eine Person einen elektronischen Geldtransfer einleiten kann. Der Begriff schließt ohne Einschränkung auch ein vorausbezahltes Zugangsinstrument ein.

Direkter kryptoanalytischer Angriff – ein RNG-Angriff, bei dem der Angreifer anhand einer Folge vergangener Werte, die von einem RNG erzeugt wurden, in der Lage ist, zukünftige RNG-Werte vorherzusagen oder zu schätzen.

Umleitungspool – die gemäß einem Beitragsplan gesammelten Gelder, die für die Finanzierung künftiger progressiver Jackpots und stufenweiser Jackpots oder für andere Zwecke verwendet werden sollen.

DNS, *Domain Name Service* – die weltweit verteilte Internet-Datenbank, die (unter anderem) Maschinennamen auf IP-Nummern und umgekehrt abbildet.

Domäne – eine Gruppe von Computern und Geräten in einem Netz, die als Einheit mit gemeinsamen Regeln und Verfahren verwaltet wird.

Verdopplung (auch bekannt als „Zocken/Risikospil“) – eine erweiterte Spielfunktion, mit der ein Spieler aktuelle Gewinne verdoppeln oder riskieren kann.

Notfallwiederherstellungsplan (*Disaster Recovery Plan, DRP*) – ein Plan zur Verarbeitung kritischer Anwendungen und zur Vermeidung von Datenverlusten im Falle eines größeren Hardware- oder Softwareausfalls oder der Zerstörung von Einrichtungen.

Effektive Bandbreite – die Datenmenge, die tatsächlich pro Zeiteinheit über ein Netzwerk übertragen werden kann. Die effektive Bandbreite im Internet ist in der Regel deutlich geringer als die Bandbreite der einzelnen Verbindungen.

Elektronischer Geldtransfer (*Electronic Funds Transfer, EFT*) (auch bekannt als „ECT“, „Electronic Credits Transfer“) – ein elektronischer Geldtransfer von einem unabhängigen Finanzinstitut auf ein Spielerkonto unter Verwendung eines Zahlungsdienstleisters. Dies schließt Automated Clearing House (ACH)-Überweisungen ein.

Verschlüsselung – die Umwandlung von Daten in eine Form, die als Chiffretext bezeichnet wird und von Unbefugten nicht ohne weiteres verstanden werden kann.

Verschlüsselungscode – ein kryptografischer Code, der verschlüsselt wurde, um den Wert des zugrunde liegenden Textes zu verschleiern.

Firewall – eine Komponente eines Computersystems oder Netzwerks, die dazu dient, unbefugten Zugriff oder Datenverkehr zu blockieren, während sie gleichzeitig die Kommunikation nach außen zulässt.

Flugschreiber – Spielerinnerungsfunktion, die verschiedene physische Aktionen des Spielers aufzeichnet und sie zeitlich mit anderen Spieleingaben wie Touchscreen-Aktivierungen, Tastendrücken usw. korreliert, um den Ausgang des Spiels besser rekonstruieren zu können. In Verbindung mit einem Spiel, das ein physisches Geschicklichkeitselement enthält, kann eine solche Funktion besonders nützlich sein, um Aspekte des Spielverlaufs aufzuzeichnen/zu dokumentieren, die sich auf die Körperlichkeit, Geschicklichkeit, Bewegungen oder Gesten eines Spielers beziehen.

Freispielmodus – ein Spielmodus, der es einem Spieler ermöglicht, an einem Spiel teilzunehmen, ohne einen Einsatz zu tätigen, hauptsächlich um die Spielmechanik zu lernen oder zu verstehen.

Spielzyklus – ein Spielzyklus ist definiert als „von Einsatz zu Einsatz“. Der Zyklus ist der Zeitraum vom ersten Einsatz bis zur endgültigen Übertragung der Guthabenanzeige des Spielteilnehmers oder das Spielerkontoguthaben bis zum Verlust aller eingesetzten Gelder.

Spielthema – das Konzept, der Gegenstand und die Methodik des Designs, um welches herum ein Spiel aufgebaut ist, einschließlich der Illustrationen, der Spielgrafiken, einer oder mehrerer Auszahlungstabellen, der Soundeffekte und der Musik.

Spiel mit Fähigkeitselementen – ein Spiel mit Wetteinsatz, bei dem das Geschick des Spielers und nicht der Zufall das Ergebnis des Spiels über einen längeren Zeitraum hinweg bestimmt. Ein Spiel mit Fähigkeitselementen enthält ein oder mehrere Geschicklichkeitselemente, die vom Spieler genutzt werden können, um die Gewinnquote zu beeinflussen.

Spielplattform – die Hardware und Software des interaktiven Spielsystems, die die gemeinsamen Funktionen für Spielangebote, Spielkonfigurationen, RNGs, Berichte usw. steuert.

Spielregeln (auch „Hausregeln“ genannt) – alle schriftlichen, grafischen und akustischen Informationen, die vom Betreiber zusammengestellt werden, um Teile der internen Kontrollen und bestimmte andere Informationen zusammenzufassen, die erforderlich sind, um die Öffentlichkeit über die Funktionalität des interaktiven Spielbetriebs zu informieren.

Spielsitzung – der Zeitraum, der mindestens dann beginnt, wenn ein Spieler ein Spiel oder eine Reihe von Spielen auf einer Spielplattform für ein bestimmtes Spielthema mit einem Einsatz beginnt und zum Zeitpunkt eines endgültigen Spielergebnisses für dieses Spiel oder diese Reihe von Spielen endet und mit der Möglichkeit für den Spielteilnehmer zusammenfällt, das Spiel zu beenden.

Geolokalisierung – Identifizierung des realen geografischen Standorts eines mit dem Internet verbundenen Remote-Spieler-Geräts.

Gruppenzugehörigkeit – eine Methode zur Organisation von Benutzerkonten in einer einzigen Einheit, wobei der Zugriff auf Systemfunktionen auf der Ebene der Einheit geändert werden kann und die Änderungen für alle der Einheit zugewiesenen Benutzerkonten wirksam werden.

Hardware-basierter RNG – ein RNG, der seine Zufälligkeit von kleinen physischen Ereignissen wie Stromkreis-Rückwirkungen, thermischem Rauschen, radioaktivem Zerfall, Photonen-Spin usw. ableitet.

Hash-Algorithmus – eine Funktion, die eine Datenkette in eine alphanumerische Zeichenkettenausgabe fester Länge umwandelt.

HTTP, Hypertext Transport Protocol – das zugrunde liegende Protokoll, mit dem festgelegt wird, wie Nachrichten formatiert und übertragen werden und welche Aktionen Server und Browser als Reaktion auf verschiedene Befehle ausführen sollen.

Kennung – jede spezifische und überprüfbare Tatsache in Bezug auf einen Spieler oder eine Gruppe von Spielern, die auf objektiven Kriterien in Bezug auf den Spieler oder die Gruppe von Spielern basiert und die verwendet werden kann, um eine vorgeschriebene Änderung an einer Spielkonfiguration vorzunehmen.

Drittanbieter zur Identitätsprüfung – eine Einrichtung, die die Identität von Personen überprüft oder Informationen zur Überprüfung der Identität bereitstellt.

IDS/IPS, Intrusion Detection System/Intrusion Prevention System – ein System, das alle ein- und ausgehenden Netzwerkaktivitäten prüft und verdächtige Muster erkennt, die auf einen Netzwerk- oder Systemangriff von jemandem hinweisen, der versucht, in ein System einzudringen oder es zu kompromittieren. In der Computersicherheit bezieht sich der Begriff „Intrusion Detection“ auf die Überwachung von Computer- und Netzwerkaktivitäten und die Analyse dieser Ereignisse, um nach Anzeichen für ein Eindringen in das System zu suchen.

Anreizgutschriften und/oder Preise (auch „Anreizprämien“ genannt) – Gutschriften und/oder Preise, die nicht in der Auszahlungstabelle eines Spiels beschrieben sind und auf vorher festgelegten Ereignissen oder Kriterien basieren, die durch die Parameter des interaktiven Spielsystems festgelegt sind. Eine Anreizprämie kann ein Werbepreis oder ein Bonuspreis sein.

Erhöhungsrage – der konfigurierbare oder fest kodierte Wert, der verwendet wird, um den progressiven Jackpot oder stufenweisen Jackpot zu erhöhen.

Stufenweiser Jackpot – ein Geldpreis oder eine „Auszahlung“, der/die sich beim Eintreten einer oder mehrerer in den Spielregeln festgelegter Bedingungen (definierter Ereignisse) erhöht. Zusätzlich zu den definierten Ereignissen ist es zulässig, dass sich die stufenweisen Jackpots auch in Abhängigkeit von den im Spiel eingesetzten Guthaben erhöhen. Ein Beispiel hierfür wäre ein stufenweiser Jackpot, der sich jedes Mal erhöht, wenn man einen bestimmten Gewinn in einem Bonus erhält.

Informationssicherheit – Schutz von Informationen und Informationssystemen vor unbefugtem Zugriff, unbefugter Nutzung, unbefugter Offenlegung, unbefugter Störung, unbefugter Änderung oder unbefugter Zerstörung, um Integrität, Vertraulichkeit und Verfügbarkeit zu gewährleisten.

Informationssicherheitsdienste – ein Unternehmen, das Verwaltungs-, Unterstützungs-, Sicherheits- oder Notfallwiederherstellungsdienste für regulierte Hardware oder Software anbietet.

Interaktive Spiele – Spiele, die unter Verwendung von Kommunikationstechnologie durchgeführt werden und bei denen ein Element des Glücks, der Geschicklichkeit oder der Strategie oder eine Kombination dieser Elemente bei der Ermittlung von Gewinnen verwendet wird, die eine Form der Aktivierung enthalten, um den Auswahlprozess einzuleiten, und die eine geeignete Methode für die Übermittlung des ermittelten Ergebnisses an das Remote-Spieler-Gerät verwenden.

Interaktives Spielsystem – die Hardware, Software, Firmware, Kommunikationstechnologie, andere Geräte sowie Betreiberverfahren, die eingesetzt werden, um die Teilnahme des Spielers am Spiel zu ermöglichen, und, falls unterstützt, die entsprechenden Geräte zur Anzeige der Spielergebnisse und anderer ähnlicher Informationen, die zur Erleichterung der Teilnahme des Spielers erforderlich sind. Das System stellt dem Spieler die Mittel zum Spielen zur Verfügung. Das System bietet dem Betreiber die Möglichkeit, Spielerkonten zu überprüfen, Spiele zu deaktivieren, verschiedene Spiel-/Finanztransaktions- und Kontoberichte zu erstellen, Ergebnisse für Live-Spiele einzugeben und alle konfigurierbaren Parameter einzustellen.

Internet – ein zusammenhängendes System von Netzwerken, das Computer auf der ganzen Welt über TCP/IP miteinander verbindet.

IP-Adresse, Internet-Protokoll-Adresse – eine eindeutige Nummer für einen Computer, mit der bestimmt wird, wohin im Internet übertragene Nachrichten zugestellt werden sollen. Die IP-Adresse ist vergleichbar mit einer Hausnummer im normalen Postsystem.

ISMS, Informationssicherheits-Managementsystem – ein definiertes, dokumentiertes Managementsystem, das aus einer Reihe von Richtlinien, Verfahren und Systemen zur Beherrschung

der Risiken für Unternehmensdaten besteht, mit dem Ziel, ein akzeptables Niveau der Informationssicherheitsrisiken zu gewährleisten.

Jackpot-Anzeige – eine Anzeige, die verwendet wird, um Informationen zum progressiven Jackpot oder stufenweisen Jackpot anzuzeigen.

Jackpot-Umleitungsschema – ein Teil der Jackpot-Beiträge wird in einen anderen Pool oder „Umleitungspool“ umgeleitet, der nach Bedarf für die Gestaltung des progressiven Jackpots oder des stufenweisen Jackpots verwendet wird (z. B. kann der Umleitungspool zum Resetwert des nächsten Jackpots addiert oder zur Auszahlung gleichzeitiger Gewinne eines Jackpots verwendet werden)

Jailbreaking – Modifizierung eines Smartphones oder eines anderen elektronischen Geräts, um die vom Hersteller oder Betreiber auferlegten Beschränkungen aufzuheben und die Installation nicht autorisierter Software zu ermöglichen.

Code – ein Wert, der verwendet wird, um kryptografische Operationen zu steuern, wie z. B. Entschlüsselung, Verschlüsselung, Signaturerzeugung oder Signaturprüfung.

Codeverwaltung – Aktivitäten, die den Umgang mit kryptografischen Codes und anderen zugehörigen Sicherheitsparametern (z. B. Passwörtern) während des gesamten Lebenszyklus der Codes umfassen, einschließlich ihrer Erzeugung, Speicherung, Einrichtung, Eingabe und Ausgabe sowie Nullstellung.

Bekannte Eingabe-Angriffe – ein RNG-Angriff, bei dem der Angreifer in der Lage ist, einen RNG zu kompromittieren, indem er den Zustand des RNG nach dem ersten Seeding bestimmt oder schätzt.

Linknutzung – die prozentuale Zeit, die eine Kommunikationsverbindung mit der Übertragung von Daten beschäftigt ist.

Einsätze auf Live-Ereignisse – eine Wette auf Live-Sportarten, Wettbewerbe, Spiele und andere von der Regulierungsbehörde genehmigte Arten von Live-Ereignissen, bei denen der Spieler Wetten auf Märkte innerhalb eines Live-Ereignisses platziert.

Live-Spiel – ein Spiel, das von einem Spielleiter (z. B. Geber, Croupier usw.) und/oder anderen Spielgeräten (z. B. automatischer Roulettekessel, Kugelgebläse, Spielgerät usw.) in einer Live-Spielumgebung durchgeführt wird, in der die Spielteilnehmer die Möglichkeit haben, den Spielverlauf zu überprüfen und Spielentscheidungen über die Spielplattform zu kommunizieren. Zu den Live-Spielen gehören unter anderem Live-Ziehungen, Live-Kartenspiele, Live-Tischspiele, Live-Keno-Spiele, Live-Bingo-Spiele und das Live-Spiel auf Spielgeräten oder anderen Spielen, die von der Regulierungsbehörde zugelassen sind.

Live-Spielumgebung – ein physischer Ort, der Live-Videostreaming-Technologie verwendet, um Live-Spiele für ein Remote-Player-Gerät bereitzustellen, das es dem Spieler ermöglicht, an live gestreamten Spielen teilzunehmen, mit Spielbetreuern zu interagieren und mit anderen Spielteilnehmern zu kommunizieren.

Standortdienstleister – ein Unternehmen, das den geografischen Standort von Personen identifiziert oder Informationen zur Identifizierung bereitstellt.

MAC, Message Authentication Code – eine kryptografische Prüfsumme über Daten, die einen symmetrischen Code verwendet, um sowohl versehentliche als auch absichtliche Änderungen der Daten zu erkennen.

Malware – ein Programm, das – in der Regel verdeckt – in ein System eingeschleust wird, um die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems des Opfers zu beeinträchtigen oder das Opfer auf andere Weise zu belästigen oder zu stören.

„Man-In-The-Middle“-Angriff – ein Angriff, bei dem der Angreifer die Kommunikation zwischen zwei Parteien, die glauben, direkt miteinander zu kommunizieren, heimlich weiterleitet und möglicherweise verändert.

Zuordnungsalgorithmus – ein Algorithmus oder eine Methode, mit der ein Wert einem Symbol oder Objekt zugeordnet wird, das für das aktuelle Spiel verwendbar und anwendbar ist (z. B. könnte der Wert 51 einem Pik-Ass zugeordnet werden).

Mechanischer RNG (auch bekannt als „Physische Zufallsgeräte“) – ein RNG, der Ergebnisse mechanisch generiert und dabei die Gesetze der Physik anwendet. Zu den Implementierungen von Live-Spielen gehören unter anderem mechanische Kessel, Trommeln, Gebläse, Mischer usw.

Nachrichtenauthentifizierung – eine Sicherheitsmaßnahme zur Feststellung der Authentizität einer Nachricht mit Hilfe eines Authentifikators innerhalb der Übertragung, der aus bestimmten vorbestimmten Elementen der Nachricht selbst abgeleitet wird.

Mobiler Code – ausführbarer Code, der von Computer zu Computer übertragen wird, darunter sowohl legitime als auch bösartige Codes wie Computerviren.

Multifaktor-Authentifizierung – eine Art der Authentifizierung, bei der die Identität eines Benutzers anhand von zwei oder mehr der folgenden Faktoren überprüft wird: Informationen, die nur dem Benutzer bekannt sind (z. B. ein Passwort, ein Muster oder Antworten auf Sicherheitsfragen); ein Gegenstand, den der Benutzer besitzt (z. B. ein elektronisches Token, ein physisches Token oder eine Identifikationskarte); biometrische Daten des Benutzers (z. B. Fingerabdrücke, Gesichts- oder Stimmerkennung).

Spiel mit mehreren Einsätzen – ein Spiel, bei dem mehrere unabhängige Einsätze gleichzeitig für die ausgeschriebenen Gewinne verwendet werden können.

Mystery-Prämie – eine Prämie, die in einem Spiel ausgezahlt wird, das nicht mit speziellen Gewinn Tabellen-Kombinationen verbunden ist.

Netzkommunikationsausrüstung (NCE, Network Communication Equipment) – ein oder mehrere Geräte, die die Datenkommunikation in einem System steuern, einschließlich, aber nicht beschränkt auf Kabel, Switches, Hubs, Router, Wireless Access Points und Telefone.

Beinahetreffer – zeigt eine besten Gewinnkombination über oder unter einer aktiven Gewinnlinie.

Nicht einsatzbezogener Kauf – ein vom Spielteilnehmer getätigter Kauf, der das Guthaben oder den Kontostand des Spielteilnehmers belastet und nur zu Unterhaltungszwecken verwendet wird. Ein nicht einsatzbezogener Kauf hat keinen Einfluss auf den Ausgang des Spiels. Ein Beispiel hierfür wäre der Kauf eines künstlerischen Attributs eines Spiels.

Betreiber – eine natürliche oder juristische Person, die ein interaktives Spielsystem betreibt und dabei sowohl die technischen Möglichkeiten des interaktiven Spielsystems als auch ihre eigenen internen Verfahren nutzt.

Überschuss – Pool, der die Beiträge enthält, die die Obergrenze des progressiven Jackpots oder des stufenweisen Jackpots überschreiten.

P2P-Spielsitzungen, Peer-to-Peer-Spielsitzungen – Umgebungen, die Spielteilnehmern die Möglichkeit bieten, mit- und gegeneinander zu spielen. In diesen Umgebungen nimmt der Betreiber in der Regel nicht als Partei an der Spielsitzung teil (z. B. Hausbank-Spiele), sondern stellt die Umgebung für die Nutzung durch seine Spielteilnehmer zur Verfügung und nimmt einen Rake, eine Provision oder eine Gebühr für diesen Dienst ein.

PAR Sheet – ein Spezifikationsblatt für ein Spiel, das die theoretische Auszahlungsquote für den Spielteilnehmer, die Trefferhäufigkeit, die Symbolkombination, die Anzahl der Walzen, die Anzahl der Guthaben, die akzeptiert werden können, und gegebenenfalls die Auflistung der Walzenstreifen enthält.

Passwort – eine Zeichenfolge (Buchstaben, Zahlen und andere Symbole), die zur Authentifizierung einer Identität oder zur Überprüfung der Zugriffsberechtigung verwendet wird.

Zahlungsdienstleister – ein Unternehmen, das die Einzahlung von Geldern auf Spielerkonten oder die Auszahlung von Geldern von Spielerkonten direkt ermöglicht.

Auszahlungstabelle – das mathematische Verhalten eines Spiels, das auf den Daten aus dem PAR Sheet des Herstellers basiert, einschließlich des Prozentsatzes der Auszahlungsquote, und das alle möglichen Auszahlungen/Gewinne enthält.

Perfecta (auch „Exacta“ genannt) – eine Wette, bei der der Spieler in der richtigen Reihenfolge auf den ersten und zweiten Platz in einem Wettbewerb setzt.

Persistenz-Spiel – ein Spiel, das mit einem eindeutigen Attribut verbunden ist (z. B. Spieler-ID, Spiel Thema/ID der Auszahlungstabelle usw.) und eine Funktion enthält, die einen Fortschritt in Richtung der Gewährung von Spielverbesserungen und/oder Boni durch das Erreichen eines bestimmten Spielergebnisses ermöglicht.

Physik-Engine – spezialisierte Software, die sich an die physikalischen Gesetze für die Elemente oder Objekte eines Spiels annähert, einschließlich Verhaltensweisen wie Bewegung, Schwerkraft,

Geschwindigkeit, Beschleunigung, Masse usw. Die Physik-Engine wird verwendet, um Spielelemente/Objekte beim Rendern von Computergrafiken oder Videosimulationen in den Kontext der physischen Welt zu stellen.

Personenbezogene Daten – sensible Informationen, die zur Identifizierung eines bestimmten Spielteilnehmers verwendet werden können. Beispiele hierfür sind der gesetzliche Name, das Geburtsdatum, der Geburtsort, die Sozialversicherungsnummer (oder eine gleichwertige behördliche Identifikationsnummer), die Führerscheinnummer, die Reisepassnummer, die Wohnanschrift, die Telefonnummer, die E-Mail-Adresse, die Debitkartennummer, die Kreditkartennummer, die Bankkontonummer oder andere personenbezogene Informationen, sofern von der Regulierungsbehörde festgelegt.

PIN, *persönliche Identifikationsnummer* – ein numerischer Code, der einer Person zugeordnet ist und den sicheren Zugang zu einem Bereich, Konto, Netzwerk, System usw. ermöglicht.

Play from Save (vom gespeicherten Spielstand weiterspielen) – eine Funktion, die in einigen persistenten Spieldesigns verwendet wird, bei denen die Komplexität zunimmt oder zusätzliche Elemente zum Spiel hinzugefügt werden, wenn das Spiel fortgesetzt wird. Der Spielteilnehmer kann den Fortschritt speichern und das Spiel am gespeicherten Spielstand fortsetzen.

Spielerkonto (auch bekannt als „Wettkonto“) – ein für einen Spielteilnehmer geführtes Konto, auf dem Informationen zu Spiel- und Finanztransaktionen im Namen des Spielteilnehmers aufgezeichnet werden, einschließlich, aber nicht beschränkt auf Einzahlungen, Auszahlungen, Einsätze, Gewinne und Kontostandsanpassungen. Der Begriff umfasst nicht ein Konto, das ausschließlich von einem Betreiber verwendet wird, um Bonuspunkte oder -gutschriften oder ähnliche Leistungen zu erfassen, die ein Betreiber einem Spielteilnehmer gewährt und gegen Waren und/oder Dienstleistungen eingelöst werden können.

Spieler-Interaktionsgerät – ein internes oder externes Gerät, das an eine Maschine angeschlossen wird und verschiedene Arten von Spielereingaben registriert, die es dem Spielteilnehmer ermöglichen, mit der Maschine zu interagieren. Einige Beispiele sind Touchscreens, Joysticks, Handheld-Controller, Kamerasysteme usw. Das Spieler-Interaktionsgerät kann fest verdrahtet oder drahtlos sein. Ein „smarter“ Spieler-Interaktionsgerät unterstützt die Zwei-Wege-Kommunikation mit der Spielplattform. Für die Zwecke dieses technischen Standards ist eine herkömmliche Tastatur von dieser Definition ausgeschlossen, es sei denn, sie wird verwendet, um das Ergebnis eines Spiels zu beeinflussen.

Spielerschnittstelle – eine Schnittstellenanwendung oder ein Programm, über das der Benutzer die Spielersoftware ansieht und/oder mit ihr interagiert, um Aktionen an das interaktive Spielsystem zu übermitteln.

Spielertreueprogramm – ein Programm, das Anreize für Spieler auf der Grundlage des Spielvolumens oder der von einem Spieler erzielten Einnahmen bietet.

Spieler-Software – die Software, die zur Teilnahme an Spiel- und Finanztransaktionen mit dem interaktiven Spielsystem verwendet wird, die je nach Design auf das Remote-Spieler-Gerät

heruntergeladen oder installiert wird, vom interaktiven Spielsystem ausgeführt wird, auf das das Remote-Spieler-Gerät zugreift, oder eine Kombination aus beidem. Beispiele für Spieler-Software sind proprietäre Softwarepakete zum Herunterladen, HTML, Flash etc.

Pool – ein angesammeltes Reservoir von Geldbeiträgen für progressive oder stufenweise Jackpots.

Port – ein physischer Eingangs- oder Ausgangspunkt eines Moduls, der den Zugang zum Modul für physische Signale ermöglicht, die durch logische Informationsflüsse dargestellt werden (physisch getrennte Ports teilen sich nicht denselben physischen Pin oder Draht).

Prepaid-Zugangsinstrument – eine Karte, ein Code, eine elektronische Seriennummer, eine mobile Identifikationsnummer, eine persönliche Identifikationsnummer oder ein ähnliches Gerät, das in Verbindung mit einem interaktiven Spielsystem verwendet wird und dem Spieler den Zugang zu Guthaben ermöglicht, die im Voraus bezahlt wurden und zu einem bestimmten Zeitpunkt in der Zukunft durch ein solches Gerät abgerufen oder übertragen werden können.

Profiling – jede Form der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass aus verschiedenen Quellen gesammelte personenbezogene Daten verwendet werden, um bestimmte persönliche Aspekte in Bezug auf eine natürliche Person zu bewerten, insbesondere um Aspekte im Zusammenhang mit der wirtschaftlichen Lage, den persönlichen Vorlieben, Interessen, der Zuverlässigkeit, dem Verhalten, dem Standort usw. dieser natürlichen Person zu analysieren oder vorherzusagen.

Proxy – eine Anwendung, die die Verbindung zwischen Client und Server „unterbricht“. Der Proxy akzeptiert bestimmte Arten von Datenverkehr, der in ein Netzwerk ein- oder ausgeht, verarbeitet diesen und leitet ihn weiter. Auf diese Weise wird der direkte Weg zwischen dem internen und dem externen Netz effektiv geschlossen. Dadurch wird es für einen Angreifer schwieriger, an interne Adressen und andere Details des internen Netzes zu gelangen.

Progressiver Jackpot – ein Geldpreis oder „Auszahlungsbetrag“, der je nach dem im Spiel eingesetzten Guthaben ansteigt.

Angebotsprämie – eine Anreizprämie, die auf vordefinierten Spieleraktivitätskriterien basiert, die an ein bestimmtes Spielerkonto gebunden sind und im Allgemeinen wiederkehren. Beispiele hierfür sind das Sammeln von eingeschränkten Gutschriften, die mit der ersten Einzahlung übereinstimmen, die Vergabe von Punkten für einen bestimmten Guthabenbetrag, der in einem Spiel gespielt wurde, die Vergabe von Guthaben für das Setzen eines Betrags, der über einem bestimmten Guthabenbetrag liegt, innerhalb eines bestimmten Zeitraums.

Proposition-Spieler – ein Spieler, der für die Teilnahme an einem Spiel angeheuert wurde und sein eigenes Geld einsetzt.

Protokoll – eine Reihe von Regeln und Konventionen, die den Informationsaustausch zwischen Geräten über ein Netz oder andere Medien spezifizieren.

Quinella – eine Wette, bei der die ersten beiden Plätze in einem Wettbewerb vorhergesagt werden, aber nicht notwendigerweise die Reihenfolge der Platzierung.

Rake, Provision oder Gebühr – ein Betrag, der vom Betreiber vom Gesamtbetrag der Wetteinsätze eines Spiels einbehalten und nicht ausgeschüttet wird.

Fernzugriff – jeder Zugriff von außerhalb des Systems oder Systemnetzwerks, einschließlich des Zugriffs von anderen Netzwerken innerhalb desselben Standorts oder Austragungsortes.

Remote-Spieler-Gerät – ein Gerät im Besitz des Spielers, das zumindest für die Ausführung des Spiels verwendet wird. Beispiele für ein Remote-Spieler-Gerät sind ein PC, ein Mobiltelefon, ein Tablet usw.

Rücksetzwert – der für einen progressiven Jackpot oder einen stufenweisen Jackpot anfänglich angebotene Betrag, bevor dieser sich erhöht.

Eingeschränkte Anreizgutschriften (auch bekannt als „nicht auszahlbare Anreizgutschriften“) – Bonusgutschriften, die entweder keinen Auszahlungswert haben oder erst dann ausgezahlt werden können, wenn eine Umsatzanforderung oder andere mit den Gutschriften verbundene Einschränkungen erfüllt sind.

Eingeschränkte Spielerguthaben – Spielerguthaben, die nicht gegen Bargeld eingelöst werden können, einschließlich eingeschränkter Anreizgutschriften.

Risiko – die Wahrscheinlichkeit, dass eine Bedrohung bei ihrem Angriff auf ein Netzwerk oder System erfolgreich ist.

Zufallszahlengenerator (RNG, Random Number Generator) – ein rechnerisches oder physisches Gerät, ein Algorithmus oder ein System, das so konzipiert ist, dass es Zahlen in einer Weise erzeugt, die von einer Zufallsauswahl nicht zu unterscheiden ist.

RNG-Zeitraum – die Länge der geordneten Folge von Rohzahlen, die vom Zufallszahlengenerator ausgegeben werden. Wenn der Zufallszahlengenerator zyklisch ist, gilt er als endlich. Andernfalls ist er unendlich.

RNG-Status – der Status, der durch eine oder mehrere Variablen im Computerspeicher definiert ist und einen bestimmten Punkt im Zyklus des Zufallsgenerators darstellt. Der RNG-Status kann geändert werden, indem eine oder mehrere dieser Variablen durch neue Werte ersetzt werden oder die Werte auf andere Weise mit neuen Daten gemischt werden.

Rooting – Erlangung von Root-Zugriff auf den Code des Betriebssystems, um den Softwarecode auf dem Mobiltelefon oder einem anderen Remote-Spieler-Gerät zu ändern oder Software zu installieren, deren Installation der Hersteller nicht zulassen würde.

Auszahlungsquote (RTP, Return to Player) – ein Verhältnis zwischen dem „Gesamtgewinn“ und dem „Gesamteinsatz“ eines Spielteilnehmers. Ein solcher Ertrag kann „theoretisch“ (auf der

Grundlage mathematischer Berechnungen oder Simulationen) oder „tatsächlich“ (auf der Grundlage der von einem aktivierten Spiel unterstützten Messung) sein.

Skalierungsalgorithmus – ein Algorithmus oder eine Methode, mit der die von einem Zufallsgenerator ausgewählten Zahlen für die Verwendung im Spiel von einem größeren Bereich auf einen kleineren Bereich skaliert oder abgebildet werden.

Sicheres Kommunikationsprotokoll – ein Kommunikationsprotokoll, das einen angemessenen Schutz der Vertraulichkeit, Authentifizierung und Integrität des Inhalts bietet.

Sicherheitszertifikat – Informationen, oft als Textdatei gespeichert, die vom Transport Socket Layer (TSL)-Protokoll zum Aufbau einer sicheren Verbindung verwendet werden. Damit eine TSL-Verbindung hergestellt werden kann, müssen beide Seiten über ein gültiges Sicherheitszertifikat verfügen.

Sicherheitsrichtlinie – ein Dokument, das die Struktur des Sicherheitsmanagements abgrenzt, die Verantwortlichkeiten für die Sicherheit klar zuweist und die Grundlage für eine zuverlässige Messung des Fortschritts und der Einhaltung der Vorschriften schafft

Seeding / Seed – die Initialisierung der Zustandsvariablen eines Zufallsgenerators. Der für die Initialisierung verwendete Quellwert oder die Quellwerte bezeichnet man als Seed.

Sensible Informationen – Informationen wie personenbezogene Daten, Spieldaten, Validierungsnummern, Authentifizierungsnachweise, PINs, Passwörter, sichere Seeds und Codes sowie andere Daten, die auf sichere Weise behandelt werden müssen.

Server – eine laufende Instanz von Software, die in der Lage ist, Anfragen von Clients zu akzeptieren, und der Computer, der diese Software ausführt. Server arbeiten innerhalb einer Client-Server-Architektur, in der „Server“ Computerprogramme sind, die laufen, um die Anfragen anderer Programme („Clients“) auszuführen. In diesem Fall wäre der „Server“ das interaktive Spielsystem und die „Clients“ wären die Remote-Spieler-Geräte.

Shellcode – ein kleines Codestück, das als Nutzlast bei der Ausnutzung von Sicherheitslücken verwendet wird. Ein Shellcode nutzt eine Schwachstelle aus und gibt einem Angreifer die Möglichkeit, die Informationssicherheit eines Systems zu verringern.

Shill – ein Spieler, der angeheuert wurde, um an einem Spiel teilzunehmen, und im Namen des Betreibers Geld einsetzt.

Mischalgorithmus – ein Algorithmus oder eine Methode, bei der die Ausgabe des Zufallsgenerators verwendet wird, um ersatzlose Daten zu erzeugen, oder, gleichwertig, um die Reihenfolge mehrerer Objekte zufällig zu bestimmen. Alle möglichen Reihenfolgen sollten gleich wahrscheinlich sein.

Soft-Play – eine Absprachemethode, bei der ein oder mehrere Spielteilnehmer darauf verzichten, gegen einen anderen Spielteilnehmer zu spielen, wenn ein solches Verhalten nach den normalen

Spielpraktiken unangemessen ist (z. B. wenn ein Spielteilnehmer das Spiel verlässt, obwohl der Sieg sicher ist).

Software-basierter RNG – ein Zufallsgenerator, der seine Zufälligkeit von einem computer- oder software-gestützten Algorithmus ableitet.

Quellcode – eine Textauflistung von Befehlen, die zu einem ausführbaren Computerprogramm kompiliert oder zusammengestellt werden.

Startwert – der anfängliche Wert des progressiven oder stufenweisen Jackpots (umfasst nicht die Werte aus Überschuss- oder Umleitungspools).

State Compromise Extension-Angriff – ein Angriff auf den Zufallsgenerator, bei dem ein Angreifer einen einzelnen Zustand des Zufallsgenerators kompromittiert und mit dieser Information in vergangene oder zukünftige Ausgaben des Zufallsgenerators eindringt. Normalerweise wird dieser Angriff mit dem Seed-Status oder einem verwundbaren Status ausgeführt, in dem nicht ausreichend Entropie verfügbar ist.

Zustandsloses Protokoll – ein Kommunikationsschema, bei dem jede Anfrage als unabhängige Transaktion behandelt wird, die in keinem Zusammenhang mit einer früheren Anfrage steht, so dass die Kommunikation aus unabhängigen Paaren von Anfragen und Antworten besteht.

Aufgabe – eine Option, die bei einigen Kartenspielen zur Verfügung steht und bei der der Spieler die Hälfte seines Einsatzes einbüßen kann, anstatt seine aktive Hand auszuspielen. Es gibt zwei Arten der Aufgabe: früh und spät. Diese Begriffe beziehen sich darauf, ob der Geber prüft, ob er einen Blackjack hat oder nicht (wenn ein Ass oder eine 10 aufgedeckt wird), bevor der Spieler die Entscheidung zur Aufgabe trifft.

Systemadministrator – die Person(en), die für die Aufrechterhaltung des stabilen Betriebs des interaktiven Spielsystems (einschließlich Software- und Hardware-Infrastruktur und Anwendungssoftware) verantwortlich ist/sind.

TCP/IP, Transmission Control Protocol/Internet Protocol – eine Reihe von Kommunikationsprotokollen, die zur Verbindung von Hosts im Internet verwendet werden.

Drittanbieter – ein Unternehmen, das im Namen eines Betreibers handelt, um Dienstleistungen zu erbringen, die für die allgemeine Durchführung interaktiver Spiele genutzt werden.

Bedrohung – jeder Umstand oder jedes Ereignis mit dem Potenzial, den Netzwerkbetrieb (einschließlich Auftrag, Funktionen, Image oder Reputation), Vermögenswerte oder Einzelpersonen über ein System durch unbefugten Zugriff, Zerstörung, Offenlegung, Änderung von Informationen und/oder Dienstverweigerung zu beeinträchtigen. Sowie das Potenzial, dass eine Bedrohungsquelle erfolgreich eine Systemschwachstelle ausnutzt.

Zeitstempel – eine Aufzeichnung des aktuellen Werts von Datum und Uhrzeit des interaktiven Spielsystems, die einer Nachricht zum Zeitpunkt ihrer Erstellung hinzugefügt wird.

Touchscreen – ein Videobildschirm, der durch elektrische Berührungspunkte auf dem Bildschirm auch als Eingabegerät für den Spieler dient.

Turnier (auch „Wettbewerb/Turnier“ genannt) – ein organisiertes, überwacht Ereignis, das es einem Spielteilnehmer ermöglicht, gegen andere Spielteilnehmer anzutreten. Bei einem Turnier ohne Geldeinsätze wird nur mit Turniergeuthaben oder Punkten gespielt, die keinen Geldwert haben. Im Gegensatz dazu ermöglicht ein Turnier mit Geldeinsätzen das Spielen mit Einsätzen in Verbindung mit der Durchführung des Turniers.

Trifecta – eine Wette, bei der ein Spieler gewinnt, indem er die drei Erstplatzierten eines Wettbewerbs in der richtigen Reihenfolge auswählt.

Unbefugter Zugriff – eine Person verschafft sich ohne Erlaubnis logischen oder physischen Zugriff auf ein Netzwerk, ein System, eine Anwendung, Daten oder eine andere Ressource.

Uneingeschränkte Anreizgutschriften (auch „auszahlbare Anreizgutschriften“ genannt) – Anreizgutschriften, die gegen Bargeld eingelöst werden können.

Uneingeschränkte Spielerguthaben – Spielerguthaben, die gegen Bargeld eingelöst werden können, einschließlich eingeschränkter Anreizgutschriften.

Versionskontrolle – die Methode, mit der überprüft wird, ob ein sich entwickelndes, genehmigtes interaktives Spielsystem in einem genehmigten Zustand funktioniert.

Wetten auf virtuelle Ereignisse – eine Form des Wettens, die die Platzierung von Wetten auf Sportarten, Wettbewerbe und Spiele ermöglicht, deren Ergebnisse ausschließlich durch einen genehmigten Zufallszahlengenerator (RNG) bestimmt werden.

Virtueller Gegner – ein computergestützter Spieler, der mit Geschick an einem Spiel teilnimmt und die Aktionen eines echten Spielers effektiv nachahmt.

Virus – ein sich, in der Regel mit böswilligen Absichten, selbst replizierendes Programm, das ausgeführt wird und sich verbreitet, indem es andere Programme oder Dateien modifiziert.

Virenschanner – Software zur Verhinderung, Erkennung und Entfernung von Computerviren, einschließlich Malware, Würmern und Trojanern.

Virtuelles Privates Netzwerk (VPN) – ein logisches Netzwerk, das über ein bestehendes physisches Netzwerk aufgebaut wird und in der Regel nicht alle Knoten des physischen Netzwerks umfasst.

Schwachstelle – Software, Hardware oder andere Schwachstellen in einem Netz oder System, die eine „Tür“ zur Einschleusung einer Bedrohung darstellen können.

Einsatz – jeder Einsatz von Guthaben oder Gutschriften durch den Spieler, der einen Einfluss auf das Spielergebnis hat.

Wi-Fi – die Standardtechnologie für drahtlose lokale Netzwerke (WLAN) zur Verbindung von Computern und elektronischen Geräten untereinander und/oder mit dem Internet.